A character formula for the Sidelnikov-Lempel-Cohn-Eastman sequences

by
Goldwyn Millar
B.Sc, M.Sc. (University of Manitoba)

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

in
School of Mathematics and Statistics
Ottawa-Carleton Institute for Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada

©Copyright
2014-2017, Goldwyn Millar

Abstract

We obtain a formula expressing the character values of the almost difference sets associated with the Sidelnikov-Lempel-Cohn-Eastman (SLCE) sequences in terms of certain Jacobi sums. As a result, we are able to obtain new insight into the pseudo-randomness properties of the SLCE sequences.

We consider the problem of determining maximal sets of shift-inequivalent decimations of SLCE sequences, or rather the equivalent problem of determining the multiplier groups of the SLCE almost difference sets. Using our character formula in conjunction with some tools from algebraic number theory (such as Stickelberger's Theorem) we obtain a numerical necessary condition for a residue to be a multiplier of an SLCE almost difference set. We use this necessary condition to prove that if p is a prime congruent to 3 modulo 4, the multiplier group of an SLCE almost difference set over the prime field of order p must be trivial. Consequently, we obtain families of shift-inequivalent decimations of SLCE sequences.

We also consider the problem of determining the linear complexity of the SLCE sequences. Due to certain technical considerations, this problem is rather difficult and has resisted the efforts of a number of mathematicians over the past 15 years. Making use of our character formula together with explicit evaluations of Jacobi sums in the pure and small index cases, we obtain new upper bounds on the linear complexity of these sequences.

Contents

Symbol Index

Chapter 1

Introduction

I

In this chapter, we give an overview of the contents of this thesis. However, we wish to begin by making a quick note for the reader. We have found it necessary to include a large amount of expositional material in this document, so for the sake of clarity, we have labelled the sections including original work with a $*$. In a few of these sections, the original work amounts to little more than routine extensions of known results; however, other sections include ideas which, we hope, are at least somewhat novel. In Section 4.4, we present the character formula that forms the basis of all of our original work in this thesis. We deduce consequences of this formula in Sections 5.1, 5.2, and 6.2. Besides the character formula given in Section 4.4, we consider the necessary condition for a residue to be a multiplier of an SLCE almost

difference set proven in Section 5.1 to be our most mathematically interesting result.

II

It has long been known that periodic binary sequences possessing certain special properties have applications in electrical engineering. These applications include the generation of secure key-streams for use in stream-cipher cryptography as well as the design of signals for use in RADAR and direct sequence spread spectrum radio communication systems (see, for instance, [92], [39, Section 5.1 and Chapter 12], and [42, Section 1.5]).

In a 1955 report for the Glenn L. Martin company, Solomon Golomb identifies several properties a sequence might possess that would render it optimal for use in cryptographic applications [37]; he claims that, ideally, a sequence would be balanced, have nearly ideal autocorrelation, and possess the run property. Since Golomb's report, several other desiderata have been identified. In order to be cryptographically secure, a sequence must have large linear complexity [42, Chapter 15]. For direct sequence spread spectrum applications, one would like to have families of sequences with low cross-correlation [39, Section 5.1 and Chapter 12].

Many classes of sequences possess some desirable properties, but no known class possesses all of them. The well-known m-sequences have all three of Golomb's pseudo-randomness properties [39, Section 5.2]. However, they

also have small linear complexity and so are not suitable for direct use in cryptographic applications.

In some cases, it is still an open question whether or not a class of sequences possesses a given property. Thus, researchers focus both on searching for new sequences with desirable properties and on studying the properties of known classes of sequences. In this thesis, we analyze a class of sequences that were originally discovered by Sidelnikov [86] and then independently rediscovered by Lempel, Cohn, and Eastman [62]. We shall refer to these sequences as the Sidelnikov-Lempel-Cohn-Eastman (SLCE) sequences. The SLCE sequences are balanced and have nearly optimal autocorrelation. It is therefore of interest to determine whether they have other desirable properties as well (so that one can judge whether they might be useful in applications).

III

The existence of periodic binary sequences with nice autocorrelation properties is equivalent to the existence of certain combinatorial objects. Depending on the sequences in question, these combinatorial objects might be difference sets or almost difference sets (both of which are special types of subsets of finite groups). Group characters are a useful tool for studying difference sets and almost difference sets: making use of characters, one can show that the existence of a difference set or an almost difference set is equivalent to the

existence of an integer in a cyclotomic field satisfying certain equations (see, for instance, [12, Section VI.3] and [6]). Thus, tools from algebraic number theory can be brought to bear on questions concerning these combinatorial objects.

IV

Gauss and Jacobi sums are special types of character sums defined on finite fields. These sums have numerous interesting applications, both in number theory and in information theory (see, for instance, [11, Chapters 3, 4, and 11] and [53, Chapters 6 and 8]). It turns out that the character values of two important classes of difference sets can be expressed in terms of Gauss and Jacobi sums; indeed, we discuss these character evaluations in Section 4.4 of this thesis.

We prove a new formula that expresses the character values of the almost difference sets associated with the SLCE sequences in terms of certain Jacobi sums. This formula, which is also discussed in Section 4.4, is the fundamental tool in our investigation of the SLCE sequences.

V

By applying special types of transformations, it is sometimes possible to use a single sequence to generate a family of sequences with desirable proper-

ties. One such transformation is a called a decimation. For instance, the sets consisting of all shift-inequivalent decimations of an m-sequence are somewhat nice families of sequences: they have the virtue that each sequence they contain has nearly ideal autocorrelation. Despite the fact that m-sequences have been studied since the 50s, it is still an open problem to determine the cross-correlation properties of these families of sequences [42, Section 10.6].

One can also obtain other families of sequences from the m-sequences. For instance, the Gold sequence family consists of term-wise sums of m-sequences with shifts of decimations of m-sequences. It is known that the Gold family has nice cross-correlation properties but that the sequences in this family have worse autocorrelation than the m-sequences themselves [39, Section 10.2]. Interestingly, the Gold sequences are currently used in the civilian C/A code for the US Global Positioning System (see [42, Section 11.2, Exercise 2]).

It is also possible to generate sequence families from the SLCE sequences (see, for instance, [23], [24], and [40]). However, prior to our work in this thesis, very little was known about which decimations of SLCE sequences give rise to shift-inequivalent sequences. We make significant progress towards solving this problem using our character formula in conjunction with some tools from algebraic number theory, such as Stickelberger's Theorem (which gives the prime ideal factorizations of the ideals generated by Gauss or Jacobi sums in rings of cyclotomic integers). In particular, we give an easily checkable numerical sufficient condition that enables one to determine

whether or not two decimations of an SLCE sequence are shift inequivalent. Furthermore, using this tool, we are able to completely specify maximal sets of shift-inequivalent decimations of SLCE sequences in an important special case. Thus, we obtain new sequence families, each of whose members has nearly ideal autocorrelation. If it turns out that these sequence families have low cross-correlation, then they could be useful in applications.

The constructions of the other known families of sequences that can be generated from the SLCE sequences are similar in spirit to the construction of the Gold sequences from the m-sequences: they are obtained by forming term-wise sums of SLCE sequences with shifts of SLCE sequences (or shifts of decimations of SLCE sequences). Furthermore, the relation of our new families to these other Sidelnikov families is similar to the relation of the families of shift-inequivalent decimations of m-sequences to the families of Gold sequences. The other Sidelnikov families are larger and are known to have good cross-correlation properties (whereas the cross-correlation properties of our families are as of yet unknown) but our families do have the virtue that each sequence they contain has nearly ideal autocorrelation.

VI

We also use our theoretical framework to investigate another property of the SLCE sequences. It is an important open problem to determine the linear complexity of these sequences. However, due to technical considerations, this problem seems to be quite difficult and so has resisted the attempts of a number of mathematicians over the past 15 years. We are able to make some progress towards determining the linear complexity of the SLCE sequences using our character formula in conjunction with explicit evaluations of Gauss sums in the pure and small index cases. We discuss our new results in this direction in Chapter 6.

VII

A number of interesting questions about Sidelnikov sequences remain open. Furthermore, although we have made progress towards solving some of these problems, the results from this thesis also point towards new open problems. Possible directions for future work are discussed in Chapter 7.

Chapter 2

Feedback shift register sequences and their applications

In this chapter, we discuss feedback shift register sequences in detail. We begin with the application that motivated the study of these sequences in the first place: the problem of generating secure key streams for use in stream cipher cryptography. In particular, we introduce feedback shift registers and discuss the properties that make sequences useful for cryptographic applications. Next, we explore the use of feedback shift register sequences in direct sequence spread spectrum applications. Finally, we give an overview of the well-known m-sequences (and some related sequence families) as well as a thorough discussion of the SLCE sequences.

2.1 Stream-cipher cryptography

2.1.1 Private key crypto-systems

Suppose that a sender A wishes to send a secret message to a receiver B over an insecure channel. One type of scheme for accomplishing this task is a private key (or symmetric) crypto-system. In such a scheme, both A and B are in possession of a secret key; A encrypts a message using the key and sends it to B, who then decrypts the message using the same key (or some simple transformation of that key). Note that in order for such a system to be secure, the secret key would need to have been communicated from A to B (or vice-versa) over a secure channel.

Symmetric crypto-systems have been in use since antiquity. Julius Caesar used a simple private key crypto-system to encrypt his messages: he replaced each letter he wanted to send with the letter appearing three spaces to the left in the alphabet. For instance, he would replace D by A, he would replace B by Y, and so forth. Caesar's crypto-system likely worked well at the time but would not provide much protection from modern cryptanalysis (see [79, Section 3.1.1]).

A more sophisticated historical example is provided by the Enigma machines that were used by Nazi Germany to encode secret messages during World War II (see, for instance, [19, Chapter 9]). These machines generated a type of cipher in which the letters of a plaintext message were replaced, seemingly at random, by different letters: for each letter in the message, the

machines would pseudorandomly generate a permutation of the alphabet and would then apply that permutation to the letter in question. The Enigmas applied different permutations to each of the different letters appearing in a message.

Through the joint efforts of Polish, French, British, and American cryptographic agencies, the Allies were able to decipher many of the messages sent by the Enigma machines. The intelligence gleaned from these messages is thought to have played an important role in determining the outcome of the war [96].

The following model, which is taken from the introduction of [92], describes (very generally) the way many modern symmetric crypto-systems work. A wants to send B the binary sequence $m_1, m_2, ...$ But, before sending this sequence, A enciphers it as follows: to each bit of the sequence, A adds the corresponding bit of the key sequence $x_1, x_2...$ (here, the addition is performed modulo 2). Then A sends B the enciphered message $c_1 = m_1+x_1, c_2 = m_2+x_2, ...$, which B in turn deciphers by adding back the key sequence bit by bit to obtain $c_1+x_1, c_2+x_2, ... = (m_1+x_1)+x_1, (m_2+x_2)+x_2, ... = m_1, m_2, ...$

Interestingly, there do exist private-key crypto-systems that are immune to even the most sophisticated cryptanalysis. In order for a symmetric crypto-system to be secure, it should be difficult for an eavesdropper to guess the original message $m_1, m_2, ...$ being sent, even if they are able to intercept the enciphered message $c_1, c_2, ...$ Now, it is possible to generate a truly random key sequence $x_1, x_2, ...$ If a key is truly random and is used only once,

the corresponding symmetric crypto-system is called a *one-time pad*. Claude Shannon proved that if a message is transmitted using a one-time pad, then the enciphered message provides no information about the original message [84].

Despite providing perfect security, one-time pads are costly to implement and so are rarely used. The main problem is that in order to use such a system, one would have to generate a sequence of random numbers as long as the plaintext message being sent, which is a computationally expensive task. As an illustrative example, following the Cuban missile crisis, a secure line of communication known as the "hotline" was set up between the Pentagon and the Kremlin, and this line of communication was encrypted using a one-time pad. However, even in this case, the one-time pad was eventually replaced by a more conventional crypto-system [82, Section 2].

In contrast to the one-time pad, many contemporary symmetric crypto-systems are inexpensive to implement but also somewhat vulnerable to attack (see [25] and [42] for general discussions of such cryptosystems). An alternative is provided by public key (or asymmetric) crypto-systems, such as the well-known RSA crypto-system. These schemes are commonly described in introductory algebra and number theory courses, and they are not salient to our work in this thesis, so we will not describe them here.

However, we do note that while public key crypto-systems are not provably unbreakable like the one-time pad, they are known to provide excellent security: for instance, there is no known method to break the RSA crypto-

system. That being said, relative to private key crypto-systems, public key crypto-systems are also rather expensive to implement (see, for example, the comparison given in [58, p.88] or the comment at the bottom of [25, p.81]). For this reason, many modern cryptographic protocols are designed using a mix of symmetric and asymmetric cryptography. A secret key is passed between A and B using an asymmetric crypto-system, and then messages are sent between A and B using a symmetric crypto-system based on that key [25, Section 4.1].

2.1.2 Feedback shift registers

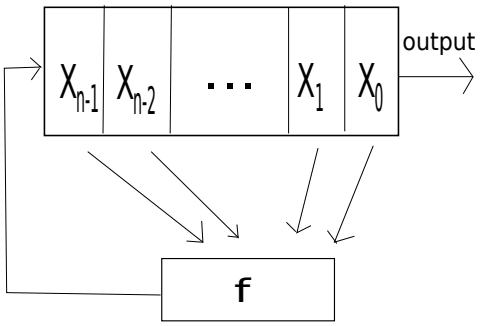
Suppose again that A wishes to send B a secret message over an insecure channel, but now assume also that it is not known in advance how long the message is going to be. For instance, A and B might be soldiers communicating to one another electronically in an unpredictable, hostile environment. Alternatively, A might be a wireless router providing an internet connection to a laptop B in a coffee shop.

In practice, there are two types of symmetric crypto-systems that are used to accomplish such a task: block-ciphers and stream-ciphers. In block-ciphers, plaintext messages are encrypted one block at a time (for blocks of bits of some fixed length). The disadvantage of such a scheme is that if the length of a plaintext message does not wind up being a multiple of the length of the blocks, then one has to add "padding" (such as a string of null bits) to the plaintext message to make it a multiple of said length, creating an

obvious inefficiency.

By contrast, in stream-ciphers, plaintext messages are enciphered one letter at a time. Key streams for stream-ciphers can be generated by machines called feedback shift registers. These devices are computationally inexpensive to implement, and they can be used to generate sequences which, although not truly random, are in a sense pseudorandom [42, Section 1.2].

An *n-stage binary shift register* is a circuit of n consecutive two-state storage units (which are called *stages*). The state of each stage is shifted to the next stage to the right at intervals regulated by a single clock. A *binary feedback shift register* is a simple machine comprised of a shift register, a feedback loop, and a mechanism for outputting binary sequences. The state of the rightmost stage is output as part of the output sequence, and the feedback loop is used to determine the state of the leftmost stage from the previous states of all n stages. The following diagram, which is essentially [39, Figure 4.1], illustrates the functionality of these machines.



The vectors of n states appearing at some point in the shift register are also called *states*. There is of course an initial state $(a_0, ..., a_{n-1})$. Furthermore, at each pulse, a new state is determined from the previous state according to the feedback loop, whose design is based on a Boolean function f of n variables called a *feedback function*. Indeed, the state following $(x_0, x_1, x_2, ..., x_{n-1})$ is $(x_1, x_2, ..., x_{n-1}, f(x_0, x_1, ..., x_{n-1}))$. Naturally, the sequence $a_0, a_1, ..., a_n, ...$ output by the feedback shift register is called a *feedback shift register sequence*.

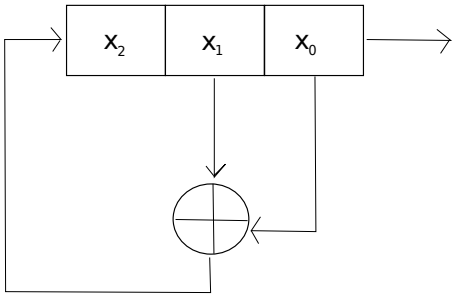
We digress to mention that it is possible to construct feedback shift registers that output sequences with elements from any finite ring [42, Section 1.2]. The design of such machines is similar to the design of the binary feedback shift registers (see, for example, [39, Section 4.1.2]). Considering

sequences defined over rings other than $\mathbb{F}_2$ opens up new possibilities for sequence design. However, feedback shift registers that generate sequences over rings other than $\mathbb{F}_2$ do generally require more circuitry to implement than binary feedback shift registers (again, see [39, Section 4.1.2]).

Let us now return to binary feedback shift registers. In the special case in which the feedback function of one of these machines a is linear function $f(x_0, ..., x_{n-1}) = q_n x_0 + ... + q_1 x_{n-1}$ (for some $q_1, ..., q_n \in \mathbb{F}_2$) we call the machine a *linear feedback shift register* (LFSR). Otherwise, we call it a *nonlinear feedback shift register* (NLFSR).

Example 2.1.1. *[This is [39, Example 4.2].] Consider the* 3 *stage LFSR with feedback function* $f(x_0, x_1, x_2) = x_0 + x_1$. *If we set the initial state of this LFSR to* 100, *then the LFSR outputs the sequence* 10010111001011...

The following diagram describes the functionality of this LFSR. Here, $\oplus$ *is used to represent a mod* 2 *adding machine.*



As is clear from the above diagram, LFSRs are particularly simple to implement in hardware. Furthermore, they can be readily analyzed mathematically (indeed, some of the basic theory of LFSRs is presented later in this chapter). By contrast, the mathematical properties of NLFSRs are not well understood (see, for instance, the comment about periods of NLFSR sequences at the bottom of [39, Section 4.1.1]).

Unfortunately, it is difficult to generate a cryptographically secure sequence using an LFSR with a reasonable number of stages. For this reason, sequence generators have been designed that make use of several LFSRs in concert; these devices combine the output sequences of their component LFSRs in various ways, thus producing cryptographically strong sequences with well-understood mathematical properties (consider, for example, the

sequence generator described in [13]).

2.1.3 Cryptographic imperatives

Notation 2.1.2. *We denote the binary sequence $a_0a_1a_2...$ by* **a**. *Suppose that there exist integers $v > 0$, $u \geq 0$ such that $a_{i+v} = a_i$ for each $i \geq u$. Then we say that* **a** *is* ultimately periodic. *The number v is called a* period *of* **a**. *When $u = 0$, we say that* **a** *is* periodic.

N.b. The least period of a sequence is sometimes referred to as the *period of the sequence.*

For example, the shift register sequence 10010111001011... from Example 2.1.1 is periodic of period 7.

The basic properties of shift-register sequences were developed by Golomb and Zierler in the 50s (see [37], [38], [39], or [100]). The following simple result establishes an important property of these sequences.

Theorem 2.1.3. *An n-stage binary feedback shift register sequence is ultimately periodic with period $v \leq 2^n$. If the feedback function of the shift register is linear, then $v \leq 2^n - 1$.*

Proof. Note that an n-stage binary shift register has 2^n possible states. But each state uniquely determines its successor. So, the first time a previous state is repeated, the output sequence starts re-cycling through an earlier period.

Furthermore, if the feedback function is linear, then the successor state to $00\cdots0$ is again $00\cdots0$. Thus, for an LFSR, $00\cdots0$ cannot be part of any nonzero period. So, an LFSR emitting a nonzero periodic sequence can cycle through at most $2^n - 1$ possible states. Hence, for these machines, $v \leq 2^n - 1$. $\square$

The most significant consequence of this result is that since feedback shift register sequences are periodic, they cannot be truly random. So, it is perhaps not surprising that in practice, the level of security achieved by stream ciphers generated by feedback shift registers falls far short of the perfect secrecy guaranteed by one-time pads [82, Chapter 6].

In [92], Wanders describes the requirements a feedback shift register sequence should meet in order to provide practical security.

> 1. Predicting the full key sequence on partial observation must be very difficult. Suppose the cryptanalyst has managed to obtain some piece of the ciphertext and corresponding plaintext. By adding $c_i \oplus m_i = x_i$, he can obtain a piece of the key sequence. It must be infeasible to calculate the key from this piece of the key sequence, or to predict the full key sequence in some other manner, without explicitly calculating the key.
>
> 2. The key sequence must appear random, i.e. the key sequence must not exhibit 'statistical regularities' that may help the cryptanalyst to restore part of the message, even though breaking the cryptogram entirely remains impossible.

We discuss Wanders' second requirement in the next two sections; subsequently, we discuss his first requirement.

2.1.4 Golomb's randomness postulates

In a 1955 report for the Glenn L. Martin company [37], Solomon Golomb states three "randomness postulates": properties a feedback shift register sequence should satisfy in order to achieve the second requirement identified by Wanders. Our discussion of the randomness postulates in this section essentially follows the exposition given in [92].

Golomb's first postulate is known as the *balance property* [39, Section 5.1].

> **R-1** [If a periodic binary sequence is to be used as a key sequence for a stream cipher, then in every period of the sequence,] the number of zeroes must be nearly equal to the number of ones. More precisely, this disparity is not to exceed one.

There is an analogue of this postulate that applies to sequences with elements from any finite ring (see [42, Section 8.2]). There is also a slightly stronger requirement one can make of a sequence: a property known as *equidistribution* (again, see [42, Section 8.2]).

In order to understand the motivation for **R-1**, consider the following example (which is taken from [92]).

Example 2.1.4. *Suppose that a key sequence is used to encipher a message*

and that roughly three quarters of the bits of the key sequence are zeroes (and the rest are ones). Assume that an eavesdropper is able to obtain the cipher-text together with a piece of the plaintext. Using this information, she will be able to calculate a piece of the key sequence. Furthermore, by examining this piece, she will likely observe that roughly one quarter of the bits are ones. She may then infer (correctly) that roughly one quarter of the bits in the entire key sequence are ones. So, even though she may still not know the key sequence, she does have some nontrivial information about it, and she might be able to use this information to recover more of the message from the cipher-text.

As the authors of [42] note, by narrowing our focus to binary sequences that satisfy **R-1**, we are already considering a very restricted set of sequences. Indeed, if a binary sequence of even period v satisfies **R-1**, then it must contain as many ones as zeroes in a given period. However, the proportion of binary sequences of period v that satisfy this condition is $\binom{v}{v/2}/2^v$, and it is a simple consequence of Stirling's formula that this expression is asymptotically equal to $\sqrt{\frac{2}{\pi v}}$.

If $\mathbf{a}$ is a binary sequence of period v, then a string of k consecutive zeroes (or ones) preceded by one (or zero) and followed by one (or zero) occurring in $\mathbf{a}$ is called a *run* of zeroes (or ones) of length k. Golomb's second postulate is known as the *run property* [39, Section 5.1].

> **R-2** [If a periodic binary sequence is to be used as a key sequence in a stream cipher, then in every period of the sequence,] half

> the runs have length one, one fourth have length two, one eigth have length three, and so on, as long as the number of runs so indicated exceeds one. Moreoever, for each of these lengths, there are equally many runs of zeroes and of ones occurring in the sequence.

There is also an analogue of this property that applies to sequences with elements from any finite ring (see [42, Section 8.2]).

Example 2.1.5. *Let us return to our previous example but abandon the assumption about the proportion of ones and zeroes. If the cryptographer who enciphered the message is to succeed in keeping his message secret from the eavesdropper, then he ought to have designed his key sequence so that it is as likely for a one occurring in the sequence to be followed by a zero as it is for it to be followed by a one. If, for instance, it's more likely that a one is followed by another one than that it is followed by a zero and the eavesdropper notices this, then she has a nontrivial piece of information that she may be able to use to recover part of the plaintext message from the cipher-text. Likewise, it should be equally likely for a string of two zeroes to be followed by a zero as it is for it to be followed by a one, and so forth.*

The *correlation* function in signal processing is a way of determining how much a signal has in common with time shifted versions of itself. Here, we just give the definition of the unnormalized periodic correlation of two binary periodic sequences. For a more general discussion of the correlation function,

see [39, Chapter 1].

Notation 2.1.6. *Let M be a positive integer. For an element a of the ring $\mathbb{Z}/M\mathbb{Z}$, let a' denote the unique positive integer less than M belonging to a.*

Let $\mathbf{a} = a_0a_1a_2\ldots$ and $\mathbf{b} = b_0b_1b_2\ldots$ be binary sequences of period v. The (periodic) correlation $\mathcal{C}_{\mathbf{a},\mathbf{b}}$ of $\mathbf{a}$ and $\mathbf{b}$ is defined as follows: for each positive integer τ,

$$\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau) := \sum_{t=0}^{v-1}(-1)^{(a_t+b_{t+\tau})'}.$$

The function $\mathcal{C}_{\mathbf{a},\mathbf{a}}$ is called the *autocorrelation* function of $\mathbf{a}$, and the values $\mathcal{C}_{\mathbf{a},\mathbf{a}}(\tau)$ for $1 \leq \tau \leq v-1$ are called the *out-of-phase* autocorrelation values of $\mathbf{a}$.

Example 2.1.7. *Consider the feedback shift register sequence* 10010111001011... *from Example 2.1.1. Let us call this sequence* $\mathbf{a}$. *Notice that we can compute (say)* $\mathcal{C}_{\mathbf{a},\mathbf{a}}(3)$ *as follows. We match up the first period of* $\mathbf{a}$ *with the period of* $\mathbf{a}$ *starting* 3 *entries from the first position and we subtract the number of pairs of non-matching bits (misses) from the number of pairs of matching bits (hits).*

$$\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{array}$$

We get $\mathcal{C}_{\mathbf{a},\mathbf{a}}(3) = hits - misses = 3 - 4 = -1$.

Golomb's third postulate is known as the *two-valued autocorrelation property* [39, Section 5.1].

R-3 [If a binary sequence $\mathbf{a}$ of period v is to be used as a key sequence for a stream-cipher, then] the autocorrelation function $\mathcal{C}_{\mathbf{a},\mathbf{a}}$ is two-valued, given by

$$\mathcal{C}_{\mathbf{a},\mathbf{a}}(\tau) = \begin{cases} v & \text{if } \tau \equiv 0 \pmod{v} \\ t & \text{if } \tau \not\equiv 0 \pmod{v}. \end{cases}$$

where t is a constant. [The out-of-phase autocorrelation values should be close to zero.] If $t = -1$ for v odd or $t = 0$ for v even, then we say that the function has an ideal two-level autocorrelation function.

For analogues of this property that apply to sequences with elements in various different finite rings, see, for instance, [39, Chapter 1] or [42, Section 8.3].

Example 2.1.8. *Let us again return to our earlier example (but forgo the assumption about the proportion of zeroes and ones). Suppose the key sequence* $\mathbf{a}$ *used to encipher the message does not have low out-of-phase autocorrelation (let us say that* $\mathcal{C}_{\mathbf{a},\mathbf{a}}(10)$ *is large). Assume the eavesdropper has obtained the following piece of ciphertext:*

$$\underline{1011}01\overline{1001}\underline{1011}10\overline{1001}0 \cdots$$

(here, the underlines and the overlines are added to emphasize strings of bits

that match up with one another).

By comparing the first string of ten elements with the following string of ten elements, the eavesdropper may notice that they match up more often than not and so (correctly) infer that $\mathcal{C}_{\mathbf{a},\mathbf{a}}(10)$ *is large. Thus, she might obtain a piece of nontrivial information about the key sequence, and she may be able to use this information to recover more of the plaintext message from the cipher-text.*

In [92], Wanders argues that the requirements in all three of Golomb's postulates can be relaxed somewhat without significant cryptographic consequences. Furthermore, he suggests replacing **R-3** with the following postulate

> **CR-3** [If a periodic binary sequence **a** is to be used as a key sequence for a stream-cipher, then] the out-of-phase values of the autocorrelation function [$\mathcal{C}_{\mathbf{a},\mathbf{a}}$] should be as close to zero as possible.

According to Wanders, "... [constructions] of key sequences with a perfect, i.e. two-valued, autocorrelation function appear to be mainly of combinatorial interest."

2.1.5 Another statistical property

In this section, we discuss another statistical regularity a sequence might posses that could render it vulnerable to cryptanalysis. We have not found a discussion like the one we give here in the literature. However, in principle,

every structural property a deterministically generated sequence possesses is a manifestation of the fact that the sequence is not truly random. Consequently, every such property represents a cryptographic weakness.

We now introduce two simple transformations, each of which can be applied to a periodic sequence to obtain another periodic sequence. Let $\mathbf{a} = a_0a_1a_2...$ be a periodic sequence, and let $t \geq 1$ be an integer. Then the *t-fold decimation* of $\mathbf{a}$ is the sequence whose ith entry is a_{ti}. Following [42, Section 10.2], we denote the t-fold decimation of $\mathbf{a}$ by $\mathbf{a}[t]$. For instance, if $\mathbf{a}$ is the m-sequence 1001011... from Example 2.1.1, then $\mathbf{a}[3] = 1110100...$,

Let $\mathbb{F}_2^\infty$ denote the vector space of binary sequences. Let L be the linear transformation from $\mathbb{F}_2^\infty$ to itself defined by the rule that for each $\mathbf{b} = b_0b_1b_2... \in \mathbb{F}_2^\infty$, $L(b_0b_1b_2b_3...) = b_1b_2b_3...$; L is called the *left shift operator*. We say that a sequence $\mathbf{b} \in \mathbb{F}_2^\infty$ is a *shift* of $\mathbf{a}$ if there exists a positive integer i such that $\mathbf{a} = L^i(\mathbf{b})$ (in this case, we also say that $\mathbf{a}$ and $\mathbf{b}$ are *shift equivalent*).

Notice that if $\mathbf{a}$ again denotes the m-sequence 1001011... from Example 2.1.1, then $\mathbf{a}[2] = 1001011 = L^0(\mathbf{a})$. So, $\mathbf{a}[2]$ and $\mathbf{a}$ are shift-equivalent (in fact, they are identical). On the other hand, it is easily checked that $\mathbf{a}$ is shift-inequivalent to $\mathbf{a}[3]$.

If $\mathbf{a}$ and $\mathbf{b}$ are sequences of period v that are shift-equivalent to one another (say, with $\mathbf{a} = L^\ell(\mathbf{b})$) then $\mathcal{C}_{\mathbf{a},\mathbf{b}}$ can be obtained from $\mathcal{C}_{\mathbf{a},\mathbf{a}}$ by a simple formula. If $\tau \geq \ell$, then $C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{a},\mathbf{a}}(\tau - \ell)$; if $\tau < \ell$, then $C_{\mathbf{a},\mathbf{b}}(\tau) = C_{\mathbf{a},\mathbf{a}}(\tau + v - \ell)$. If $\mathbf{a}$ and $\mathbf{b}$ are shift-inequivalent, then we say that $\mathcal{C}_{\mathbf{a},\mathbf{b}}$ is the

periodic cross-correlation of **a** and **b**.

Example 2.1.9. *Let us once more return to the example from the previous section but forgo all of the various assumptions made about the key sequence. Assume that the eavesdropper has obtained a piece of the cipher text of length r. Suppose that the key sequence* **a** *used to encipher the message is shift equivalent to its decimation* $\mathbf{a}[t]$*. Suppose further that t is a small number relative to r. By computing a portion of the cross-correlation of this piece of cipher text with its decimation by t, she may notice that one of the values of the cross-correlation is high. Thus, she may correctly infer that* **a** *is shift-equivalent to* $\mathbf{a}[t]$ *and she may be able to use this information to recover more of the plaintext message from the cipher-text.*

Notice that the assumption that t is small relative to r is crucial in the above example. For, if $ti > r$, then the eavesdropper would initially not be able to determine a_{ti} since she has only received the first r entries of a period of **a**. Thus, t needs to be small enough relative to r that she is able to compute enough entries of $\mathbf{a}[t]$ to suspect that **a** is shift-equivalent to $\mathbf{a}[t]$. But, if this assumption is satisfied, she likely could exploit this structural property to deduce nontrivial information about the key sequence **a**.

2.1.6 Linear complexity

In this section, we identify the property sequences must have in order to satisfy Wanders' first requirement. However, in order to explore this property

thoroughly, we need to begin by developing some of the basic theory of LFSRs.

Let **a** be a periodic binary sequence of period v. Note that **a** is necessarily a linear feedback shift register sequence since **a** can be generated by the LFSR with linear feedback function $h(x_0, ..., x_{v-1}) = x_0$ whose initial state is the first period of **a**. Of course, it is possible that **a** could also be generated by a LFSR with fewer stages.

Suppose that **a** can be generated by an n-stage LFSR with feedback function $f(x_0, ..., x_{n-1}) = q_n x_0 + \cdots + q_1 x_{n-1}$. Set $q(x) = 1 + q_1 x + \cdots + q_n x^n \in \mathbb{F}_2[x]$. Then $q(x)$ is called the *connection polynomial* of the LFSR.

For a polynomial $r(x)$ of degree m, the polynomial $r^*(x) := x^m r(1/x)$ is called the *reciprocal polynomial* of $r(x)$. We note the following useful fact about reciprocal polynomials (see [42, Lemma 3.1.5]).

Lemma 2.1.10. *Let $r(x) \in \mathbb{F}_2[x]$ have a nonzero constant term. Then $r(x)$ and $r^*(x)$ have the same degree. Furthermore, $r(x)$ factors as $s(x)t(x)$ if and only if $r^*(x)$ factors as $s^*(x)t^*(x)$.*

The reciprocal polynomial $q^*(x) = x^n + q_1 x^{n-1} + \cdots + q_n$ of $q(x)$ is called the *characteristic polynomial* of the LFSR.

It follows directly from the definition of LFSRs that for each $k \geq n$,

$$a_k = q_1 a_{k-1} + \cdots + q_n a_{k-n}. \tag{2.1.1}$$

We can rephrase this recurrence relation in terms of the left shift operator:

$$L^n\mathbf{a} = (q_1L^{n-1} + \cdots + q_{n-1}L + q_nI)\mathbf{a}. \tag{2.1.2}$$

So, we deduce that

$$q^*(L)\mathbf{a} = \mathbf{0}. \tag{2.1.3}$$

Conversely, if for some polynomial $r(x) \in \mathbb{F}_2[x]$, $r(L)\mathbf{a} = \mathbf{0}$, then $r(x)$ is the characteristic polynomial of an LFSR that generates $\mathbf{a}$.

Let I be the subset of $\mathbb{F}_2[x]$ consisting of all polynomials $r(x)$ such that $r(L)\mathbf{a} = 0$. It is easy to see that I is an ideal. Recall that since $\mathbb{F}_2$ is a field, $\mathbb{F}_2[x]$ is a PID, and every nontrivial proper ideal of $\mathbb{F}_2[x]$ is generated by a polynomial of minimal degree belonging to that ideal. Furthermore, since we are working over $\mathbb{F}_2$, every ideal has a unique such polynomial of minimal degree. We denote the polynomial that generates I as $m^*(x)$. It follows by Lemma 2.1.10 that $\mathbf{a}$ has a unique connection polynomial of least degree, namely $m(x)$, and that this polynomial divides every other connection polynomial of $\mathbf{a}$. We call $m(x)$ the *minimal polynomial* of $\mathbf{a}$. Note that the degree, ℓ, of the minimal polynomial is the number of stages in the smallest LFSR that can be used to generate $\mathbf{a}$. We refer to the number ℓ as the *linear complexity* (or, *linear span*) of $\mathbf{a}$.

Let $\mathbb{F}_2[[x]]$ denote the ring of formal power series over $\mathbb{F}_2$. We recall the following result, which describes exactly which elements of $\mathbb{F}_2[[x]]$ are invertible

(see [42, Lemma 3.4.2]).

Lemma 2.1.11. *Let* $b(x) = \sum_{i=0}^{\infty} b_i x^i \in \mathbb{F}_2[[x]]$ *be a power series. Then* $b(x)$ *is invertible in* $\mathbb{F}_2[[x]]$ *if and only if* $b_0 \neq 0$.

It follows from Lemma 2.1.11 that $1/q(x) \in \mathbb{F}_2[[x]]$.

Let $a(x) := a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{F}_2[[x]]$. Let $g(x) := \sum_{m=0}^{n-1} \left(\sum_{i=0}^{m} q_i a_{m-i}\right) x^m$. It is a simple consequence of Equation 2.1.1 that $g(x)/q(x) = a(x)$. It is not hard to prove that the converse of this result is also true (see [42, Theorem 3.5.1]).

Lemma 2.1.12. *If for some polynomials* $s(x), t(x) \in \mathbb{F}_2[x]$, $s(x)/t(x) = a(x)$, *then* $t(x)$ *is a connection polynomial for an LFSR that generates* $\mathbf{a}$, *and so* $\mathbf{a}$ *can be generated by an LFSR of length* $deg(t(x))$.

Let $r(x)/m(x) = a(x) = s(x)/t(x)$, for some $r(x), s(x), t(x) \in \mathbb{F}_2[x]$ and where, as before, $m(x)$ denotes the minimal polynomial of $\mathbf{a}$. Then, by Lemma 2.1.12, $t(x)$ is a connection polynomial of $\mathbf{a}$, and it follows that there exists $h(x) \in \mathbb{F}_2[x]$ such that $t(x) = h(x)m(x)$. Hence, $r(x)h(x)m(x) = s(x)m(x)$. So, since $\mathbb{F}_2[x]$ is an integral domain and $m(x) \neq 0$, we deduce that $s(x) = r(x)h(x)$. Therefore, if the fraction $s(x)/t(x)$ is in lowest terms, then $t(x) = m(x)$. Consequently, $m(x) = t(x)/\gcd(s(x), t(x))$.

Let $A(x) := \sum_{i=0}^{v-1} a_i x^i \in \mathbb{F}_2[x]$. Note that $a(x) = A(x)(1 + x^v + x^{2v} + \cdots) = A(x)/(1 - x^v)$. Thus, we obtain the following well-known result, which plays a crucial role in the work presented in Chapter 6 of this thesis.

Theorem 2.1.13. *The minimal polynomial of* $\mathbf{a}$ *is*

$$\frac{x^v - 1}{gcd(A(x), x^v - 1)}.$$

Consequently, the linear complexity of $\mathbf{a}$ *is* $v - deg(gcd(A(x), x^v - 1))$.

We are now in a position to explain why linear complexity is relevant to Wanders' first requirement for cryptographically secure key streams. Recall that the continued fractions algorithm is a procedure by which one can obtain a sequence of rational approximations to a given real number. These approximations are best possible in the sense that relative to the magnitudes of their denominators, they are the closest rational numbers to the real number they are approximating. The continued fractions algorithm has many interesting applications, such as generating solutions to Pell's equation and factoring large integers (see, for instance, [65, Chapter 9]).

It is possible to extend the continued fractions algorithm to many different settings. Indeed, whenever it is possible to regard the elements of a ring as having an "integer part" and a "fractional part," one can define some version of this algorithm. In particular, one can define a continued fractions algorithm on the ring of formal Laurent series in the variable x^{-1} (see [42, Appendix D.2.3]).

Now, there is a well-known procedure, called the Berlekamp-Massey algorithm, that can be used to compute the minimal polynomial of a sequence $\mathbf{a}$ by obtaining successively better approximations to $a(x) = r(x)/m(x)$ in

the ring of formal power series $\mathbb{F}_2[[x]]$. This algorithm, which was first formulated by Berlekamp [9] as a decoding algorithm for BCH codes and later reformulated by Massey as a means of cryptanalyzing stream ciphers [71], is similar to the continued fractions algorithm in the ring of formal Laurent series. For a precise account of the relation between these two algorithms, see [42, Section 15.2.4].

Recall that ℓ denotes the linear complexity of $\mathbf{a}$. The Berlekamp-Massey algorithm takes as input 2ℓ consecutive entries of $\mathbf{a}$ and outputs the minimal polynomial of $\mathbf{a}$ in quadratic time. So, if a cryptanalyst is able to intercept 2ℓ consecutive bits of a plaintext message along with the corresponding bits of the enciphered message (which has been enciphered using the key sequence $\mathbf{a}$) she will easily be able to obtain the entire key sequence and thus decipher the entire message. Consequently, in order for a sequence to satisfy Wanders' first requirement, it is necessary that it have large linear complexity. Ideally, the linear complexity of a periodic sequence should be nearly as large as its period [39, Section 5.1].

2.2 Spread spectrum communications systems

One major challenge in the design of radio communications systems is finding ways of accommodating numerous users on systems that are constrained to operate within limited bandwidths. There are several commonly used types of schemes for allocating bandwidth. One method is to simply divide up

the bandwidth so that each pair of users within the system is permanently allocated a small part of the spectrum. This is sometimes called frequency division multiplexing (see [28, Section 2.3.1]). Another approach is division by time, or time division multiplexing. For this approach, each pair of users is allocated part of the spectrum, but only for short periods of time (see [28, Section 2.3.2]).

Alternatively, one can make use of what are known as *spread spectrum* systems. In these schemes, signals are deliberately spread through all or most of the spectrum and pairs of signals are distinguished from one another via a clever use of pseudorandom sequences. Spread spectrum communications systems have several virtues, including cryptographic security and resistance to jamming (see, for instance, [90, Preface] or [75]).

Frequency hopping spread spectrum is a technique whereby signals are rapidly switched between different frequencies according to the dictates of a pseudorandom sequence known both to the sender and the receiver. Frequency hopping schemes have found numerous military applications. For instance, frequency hopping is currently employed in several US military radio communications systems (see, for example, [27] and [55]). Famously, during World War II, actress Hedy Lamarr and composer George Antheil patented a frequency hopping system for radio guided torpedoes: the pseudorandom sequences in their system assign 88 different frequencies according to the notes appearing in piano rolls [42, Section 11.9]. Lamarr and Antheil's system was never put into use; however, it is possible to design practical frequency hop-

ping systems using some of the sequences we discuss in this thesis, such as the m-sequences, which are treated in the next section (see, for instance, [42, Section 11.9]).

Direct sequence spread spectrum (DSSS) is a technique whereby signals are "modulated" (in a sense explained below) by spreading codes based on pseudorandom sequences. Perhaps the most important use of DSSS is the role it plays in the design of the Global Positioning System (GPS), which is a major navigational system owned by the US government (see, for instance, [54, Section 1.3]). A type of DSSS, called code division multiple access (CDMA), played a prominent role in the design of 3rd Generation (3G) cellular networks [39, Section 12.10]. These networks have largely been replaced (or are being replaced) by other technologies. However, some proposed schemes for 5G communications networks do incorporate certain types of CDMA [52, Section 1.1]. Of course, the landscape of communications network design is rather complex, so it is difficult to predict what role CDMA might play in future wireless communications technologies.

In order to design a DSSS system, one needs a reasonable way of measuring how much two sequences have in common with one another: periodic cross-correlation is such a measure. Let $\mathbf{a}$ and $\mathbf{b}$ be two binary sequences of period v. If the magnitude of $\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)$ is close to 0 for each $\tau \neq 0 \pmod{v}$, then $\mathbf{a}$ and $\mathbf{b}$ have almost nothing in common; if the magnitude of $\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)$ is close to v for some $\tau \neq 0 \pmod{v}$, then $\mathbf{a}$ and $\mathbf{b}$ are very nearly identical.

In DSSS, each communicator is assigned a unique m-bit chip sequence. A

communicator's chip sequence modulates the messages it sends: to transmit "1," the communicator sends its entire chip sequence, and to transmit "0," the communicator sends the complement of its chip sequence. For instance, suppose that communicator X is assigned the 7-bit chip sequence 1001011 (which is actually just the first period of the sequence from Example 2.1.1). Then, in order to send the message "101," X actually transmits

$$\underline{1001011}\overline{0110100}\underline{1001011}$$

(here, the chip sequence is underlined and its complement is over-lined).

A receiver interprets signals sent by a communicator by correlating the received input against the periodic sequence whose first period is the communicator's chip sequence. In order for a message sent by communicator A to be distinguishable from a message sent to a receiver C by another communicator (say, B) it is necessary that the periodic sequence $\mathbf{a}$ whose first period is A's chip sequence have low cross-correlation with the periodic sequence $\mathbf{b}$ whose first period is B's chip sequence. Furthermore, in order to be certain that C receives the message A intended to send, it is necessary that $\mathbf{a}$ have low out-of-phase autocorrelation (so that a time shifted version of the message sent by A is not mistaken for the actual message sent by A).

Thus, for DSSS applications, one is interested in obtaining families of periodic sequences with low out-of-phase autocorrelation and pairwise low cross-correlation. Ideally, the out-of-phase autocorrelation of the sequences

in a family should be close to 0 (although, in practice, sometimes sequences are used which have good, but nowhere near ideal, autocorrelation properties; an example is provided by the Gold sequences, which are discussed later in this chapter).

The *Welch bound* [94] is a fundamental result concerning the cross-correlation of sequences. See [42, Section 11.1] for a proof.

Theorem 2.2.1. *Let* $\mathbf{a}_1, ..., \mathbf{a}_n$ *be a set of* n *pairwise shift distinct binary sequences of (least) period* v*. For each* $\mathbf{a}_i$*, let* $\mathbf{a}_i^0, \mathbf{a}_i^1, ..., \mathbf{a}_i^{v-1}$ *denote the set of* v *cyclic shifts of* $\mathbf{a}_i$*. Let* $C_{max} := max\{\mathcal{C}_{\mathbf{a}_i^j, \mathbf{a}_s^t}(\tau) | 0 \leq \tau \leq v-1, 1 \leq i, s \leq n, i \neq s, 0 \leq j, t \leq v-1\}$*. Then* $C_{max}^2 \geq v^2(n-1)/(nv-1)$.

Since $v^2(n-1)/(nv-1) \sim v$, for large values of n, the family of sequences $\{\mathbf{a}_i^j | 1 \leq i \leq n, 0 \leq j \leq v-1\}$ will contain pairs whose cross-correlation is lower bounded (roughly) by $\sqrt{v}$. Following [39, Section 5.1], we say that a family of sequences has good cross-correlation if the pairwise cross-correlation of the sequences in the family is upper bounded by $\delta\sqrt{v} + \epsilon$, for some small, positive integers δ and ϵ.

2.3 m-sequences and related sequence families

In this section, we introduce the m-sequences as well as some closely related sequence families. The classes of sequences discussed in this section are per-

haps the best known and most useful types of sequences. However, even these sequences have their limitations. Consequently, considerable research energy continues to be spent searching for new classes of sequences and analyzing the properties of promising known classes of sequences.

In the next section, we introduce the Sidelnikov-Lempel-Cohn-Eastman sequences, which are the focus of our work in this thesis. In chapter 3, we introduce several more classes of sequences as part of our discussion of difference sets and almost difference sets.

2.3.1 m-sequences

We define m-sequences with elements from any finite field. Even though our primary interest is in binary sequences, m-sequences with elements from other finite fields serve as useful auxiliary objects for our purposes.

For a prime power q, a q-ary sequence generated by an n-stage LFSR is a *maximal length sequence* (or, m-sequence) if it has period $q^n - 1$. It follows by the obvious generalization of Theorem 2.1.3 to sequences over finite fields that $q^n - 1$ is indeed the maximum possible period for a sequence over $\mathbf{F}_q$ generated by an n-stage LFSR.

The following theorem provides the key to constructing m-sequences (see [39, Theorem 4.8]).

Theorem 2.3.1. *Let* $\mathbf{a}$ *be an LFSR sequence over* $\mathbb{F}_q$ *with minimal polynomial* $m(x)$*. Assume that* $m(x)$ *is an irreducible polynomial over* $\mathbb{F}_q$ *of degree*

n. Let α be a root of $m(x)$ in the extension field $\mathbb{F}_{q^n}$. Then the (least) period of $\mathbf{a}$ is equal to the order of α.

Thus, we can generate an m-sequence over $\mathbb{F}_q$ using an n-stage LFSR for which the corresponding characteristic polynomial is a primitive polynomial over $\mathbb{F}_q$. For instance, the binary sequence 1001011... from Example 2.1.1 is an m-sequence of period $2^3 - 1 = 7$ and has minimal polynomial $x^3 + x + 1$, which is primitive over $\mathbb{F}_2$.

It turns out that m-sequences have remarkable statistical properties. Consider the sequence 1001011... Notice that in each period of this sequence, there are four ones and three zeroes. Hence, this sequence has randomness property R-1. Furthermore, 1001011... has four runs in each period (we count the one at the beginning with the two ones at the end as a run of length three). Of these runs, half have length one and one fourth have length two. So, this sequence has randomness property R-2. Finally, 1001011... has out-of-phase autocorrelation -1. Consequently, this sequence also has randomness property R-3.

Theorem 2.3.2. *[39, Properties 5.3, 5.4, and 5.5] Every binary m-sequence has randomness properties R-1, R-2, and R-3.*

It can also be shown that q-ary m-sequences satisfy generalized versions of Golomb's randomness postulates.

Perhaps the main drawback of the m-sequences is that they have low linear complexity. Indeed, since an m-sequence generated by an n-stage LFSR

is, by definition, a sequence with the largest possible period that can be generated by an n-stage LFSR, the ratio of the linear complexity of an m-sequence to its period is as bad as possible. For this reason, m-sequences are not well-suited for direct use in cryptographic applications. However, LFSRs that generate m-sequences can be used as components of more complex sequence generators that do produce cryptographically strong sequences (see, for instance, [39, Chapter 11] and [13]).

We finish this section by introducing an alternative characterization of m-sequences. To that end, we recall some ideas from abstract algebra (for further discussion of these ideas, see [26, Section 14.2]). Let K be a field, let L be a Galois extension of K, and let $\mathrm{Gal}(L/K)$ denote the group of Galois automorphisms of L fixing K. We define the *trace* from L to K to be the map that sends each $\alpha \in L$ to the sum of its Galois conjugates:

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Note that for each $\alpha \in L$, $\mathrm{Tr}_{L/K}(\alpha)$ is fixed by every $\sigma \in \mathrm{Gal}(L/K)$. So, $\mathrm{Tr}_{L/K}(\alpha)$ is, in fact, an element of K. Furthermore, if we view both L and K as vector spaces over K, then it is easy to see that $\mathrm{Tr}_{L/K}$ is a linear transformation from L onto K. We note that if M is a Galois extension of L, then $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$.

We also introduce another map from L to K, even though we will not need it until later in this thesis. We define the *norm* from L to K to be the

map that sends each $\alpha \in L$ to the product of its Galois conjugates:

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gak}(L/K)} \sigma(\alpha).$$

Note that for each $\alpha \in L$, $\mathrm{N}_{L/K}(\alpha)$ is fixed by every $\sigma \in \mathrm{Gal}(L/K)$. So, $\mathrm{N}_{L/K}$ is, in fact, an element of K. Furthermore, the norm induces a homomorphism from the multiplicative group L^* of L to the multiplicative group K^* of K. We note that if M is a Galois extension of L, then $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$.

Now, consider the case in which $L = \mathbb{F}_{q^n}$ is a Galois extension of the finite field $\mathbb{F}_q$ (for some prime power q). We have that $\mathrm{Gal}(L/K) = \langle q \rangle$. So, for each $\alpha \in L$,

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i},$$

and

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{\frac{q^n-1}{q-1}}.$$

For future reference, we note the obvious facts that for each $\alpha \in L$, $\mathrm{Tr}_{L/K}(\alpha^q) = \mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha^q) = \mathrm{N}_{L/K}(\alpha)$. Additionally, we note that $|\mathrm{Ker}(\mathrm{Tr}_{L/K})| = q^{n-1}$.

The following theorem elucidates the connection between the trace map and m-sequences (see [39, Corollary 4.6]).

Theorem 2.3.3. *Let q be a prime power, let $\mathbf{a} = a_0a_1a_2...$ be a sequence over $\mathbb{F}_q$, let n be a positive integer, and let α be a primitive element of $\mathbb{F}_{q^n}^*$. Then*

a *is an m-sequence with period* $q^n - 1$ *if and only if there exists* $\beta \in \mathbb{F}_{q^n}^*$ *such that for each positive integer* i, $a_i = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta\alpha^i)$.

For instance, let α be a root of x^3+x+1 (over $\mathbb{F}_2$). Then α is a primitive element of $\mathbb{F}_{2^3}^*$, and the m-sequence $\mathbf{a} = a_0a_1a_2... = 1001011...$ from Example 2.1.1 is obtained by the rule the for each positive integer i, $a_i = \mathrm{Tr}(\alpha^i)$.

2.3.2 Array structure

Let q be a prime power, and let n be a positive integer. Recall that for each positive integer m, $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ if and only if $m|n$. It turns out that m-sequences have an interesting structural property that reflects this fact about finite fields.

Consider the following example. Let $q = 2$, and let $n = 6$. Since $m = 3$ divides n, it follows that $\mathbb{F}_{2^3}$ is a subfield of $\mathbb{F}_{2^6}$. Note that $x^6 + x + 1$ is a primitive polynomial of degree 6 over $\mathbb{F}_2$. Let **a** be the m-sequence with minimal polynomial x^6+x+1 and initial state 000001. We arrange the 2^6-1

entries in the first period of $\mathbf{a}$ in lexicographic order in a $(2^3-1)\times 9$ array.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Examining the columns of this array, it is apparent that besides the first column, which is all zeroes, every column is a cyclically shifted version of the first period of the m-sequence 1110100.. over $\mathbb{F}_{2^3}$.

More generally, we have the following theorem, whose proof essentially follows from the trace representation of the m-sequences and the fact that $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \circ \mathrm{Tr}_{\mathbb{F}_q^n/\mathbb{F}_{q^m}}$ (see [39, Theorem 5.2]).

Theorem 2.3.4. *Let n be a composite number, let m be a proper factor of n, and let $d = \frac{q^n-1}{q^m-1}$. Then any m-sequence over $\mathbb{F}_q$ of degree n can be arranged into a $(q^m-1)\times d$ array, where each column sequence is either a cyclic shift of the first period of some fixed m-sequence of degree m over $\mathbb{F}_q$ or a zero sequence.*

The discovery of the array structure of m-sequences is essentially due to Gordon, Mills, and Welch [41]. It is possible to exploit this array structure

to construct a class of sequences that are essentially different than the m-sequences (see [41]); the sequences so obtained are sometimes called Gordon-Mills-Welch (GMW) sequences.

2.3.3 Decimations and sequence families

In this section, we discuss how m-sequences can be used to construct families of shift-inequivalent sequences with good autocorrelation and pairwise low cross-correlation. The key to these constructions is the decimation transformation we introduced in Section 2.1.5.

Recall that the sequences in families with low cross-correlation are necessarily shift distinct. Consequently, it is natural to ask which decimations of m-sequences give rise to shift-inequivalent sequences.

Now, if $\mathbf{a}$ is an m-sequence over $\mathbb{F}_q$ with minimal polynomial $m(x)$ of degree n, then since $\mathbf{a}$ has period $q^n - 1$, it follows that every nonzero n-tuple of elements from $\mathbb{F}_q$ appears at some point in $\mathbf{a}$. Consequently, if $\mathbf{b}$ is another m-sequence of degree n that is shift equivalent to $\mathbf{a}$, then the string of the first n entries of $\mathbf{b}$ occurs at some point in $\mathbf{a}$, and the subsequent entries of both $\mathbf{a}$ and $\mathbf{b}$ are determined by the LFSR of $\mathbf{a}$. So, $\mathbf{a}$ and $\mathbf{b}$ both have $m(x)$ as their minimal polynomial. Conversely, it is easy to see that if $\mathbf{a}$ and $\mathbf{b}$ are m-sequences having the same minimal polynomial, then they are shift equivalent.

See [39, Theorem 4.12] for a proof of the following theorem.

Theorem 2.3.5. *Let $m(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n, and let s be a positive integer. Let α be a root of $m(x)$ in the extension $\mathbb{F}_{q^n}$. If $m(x)$ is the minimal polynomial of a sequence $\mathbf{a}$, then if $\mathbf{a}[s] \neq \mathbf{0}$, then the minimal polynomial of $\mathbf{a}[s]$ is equal to the minimal polynomial of α^s over $\mathbb{F}_q$.*

If $m(x)$ is a minimal polynomial of an m-sequence $\mathbf{a}$ of degree n over $\mathbb{F}_q$, then it is primitive and, consequently, irreducible. Thus, if α is a root of $m(x)$, then the set of roots of $m(x)$ is identical to the set of Galois conjugates of α. But since the Galois group of $\mathbb{F}_{q^n}/\mathbb{F}_q$ is $\langle q \rangle$, it follows by Theorem 2.3.5 that for each positive integer t, $\mathbf{a}[t]$ is shift equivalent to $\mathbf{a}$ if and only if t is a power of q. Indeed, we have the following theorem (see [42, Proposition 10.2.1]).

Theorem 2.3.6. *Let q be a prime power, and let n be a positive integer. Let $\mathbf{a}$ be an m-sequence of degree n over $\mathbf{F}_q$.*

1) *Every m-sequence of degree n over $\mathbf{F}_q$ is a shift of a decimation of $\mathbf{a}$.*

2) *The decimation $\mathbf{a}[t]$ is again an m-sequence if and only if t is relatively prime to $q^n - 1$.*

3) *The decimation $\mathbf{a}[t]$ is a shift of $\mathbf{a}$ if and only if t is a power of q.*

4) *There are $\phi(q^n - 1)/n$ shift inequivalent m-sequences of degree n over $\mathbb{F}_q$.*

Thus, the set of decimations $\mathcal{F} = \{\mathbf{a}[t]\}$ (where t ranges over a set of integers congruent to representatives of the distinct cosets of $\langle q \rangle$ in $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$) is a family of $\phi(q^n - 1)/n$ shift inequivalent m-sequences. In the case that $q = 2$, $\mathcal{F}$ is a family of binary sequences with optimal autocorrela-

tion properties. It is still an open problem to determine the precise cross-correlation values of the pairs of sequences in $\mathcal{F}$. However, cross-correlation values are known in certain special cases. If $t = 1 + q^i$ for some i, then we say that $\mathbf{a}[t]$ is a *quadratic decimation*, and the precise values taken on by the function $\mathcal{C}_{\mathbf{a},\mathbf{a}[t]}$ are known (see [32], [46], [72], and [80]; alternatively, see the discussion in [42, Section 10.6]). Also, if $t = -1$, then in some cases, the values taken on by $\mathcal{C}_{\mathbf{a},\mathbf{a}[t]}$ are known (see [60]; the results from [60] are also briefly discussed in [42, Section 10.6.4]).

Even though the cross-correlation properties of the families of shift inequivalent m-sequences are unknown in general, several researchers have used decimations of m-sequences to generate families of shift-inequivalent sequences with predictable (and reasonably good) correlation properties. We conclude this section by describing one such family.

We define the *termwise sum* of the sequences $\mathbf{a} = a_0a_1a_2...$ and $\mathbf{b} = b_0b_1b_2...$ to be the sequence whose ith term is $a_i + b_i$. Let $\mathbf{a}$ be an m-sequence of degree n over $\mathbb{F}_2$. Let $t = 1+2^i$, where $1 \leq i \leq (n-1)/2$ and $\gcd(n, i) = 1$. Let $\mathbf{b} := \mathbf{a}[t]$, so that $\mathbf{b}$ is a quadratic decimation of $\mathbf{a}$. For each $0 \leq j < 2^n-1$, let $\mathbf{s}_j := L^j\mathbf{a} + \mathbf{b}$. Then, for each j, $\mathbf{s}_j$ is called a *Gold-pair* sequence. Let $\mathcal{G}_t := \{\mathbf{s}_j | 0 \leq j < 2^n - 1\}$. Then $\mathcal{G}_t$ is called a *Gold sequence family* (this family of sequences was originally discovered by Gold [36]).

If $\mathbf{a}$ is the m-sequence 1001011... from Example 2.1.1, then since $3 = 1+2$,

we can set $\mathbf{b} = \mathbf{a}[3] = 1110100...$ So, we get that

$$\mathcal{G}_3 = \{\mathbf{s}_0 = 0111111..., \mathbf{s}_1 = 1100011..., \mathbf{s}_2 = 1011010..., \mathbf{s}_3 = 0101000...$$

$$\mathbf{s}_4 = 1001101..., \mathbf{s}_5 = 0000110..., \mathbf{s}_6 = 0010001...\}$$

It is known that $\mathcal{G}_t$ is a family of $2^n - 1$ shift-inequivalent sequences and that the cross-correlation and out-of-phase autocorrelation of any pair of sequences (or any sequence) in $\mathcal{G}_t$ is contained in the set $\{-1, -1 \pm 2^{m+1}\}$, where $i = 2m + 1$ [39, Corollary 10.1]. Thus, the Gold family is a large sequence family with good autocorrelation and cross-correlation properties. Indeed, the Gold family is currently used in the US Civilian C/A code for the Global Positioning System (see [42, Exercise 2, Chapter 11]).

There are several other decimations that can be used to create sequence families in lieu of the quadratic decimations used in the construction of the Gold families (see [39, Section 10.2] for a discussion of the sequence families so obtained). It is also possible to construct families of sequences of period 2^n using similar techniques (see, for instance, the discussion of the Kasami sequences in [39, Section 10.3]).

2.4 Sidelnikov Sequences

We now discuss another class of sequences, which are similar to the m-sequences in that their definition relies on both the multiplicative and ad-

ditive structures of finite fields. Let p be an odd prime, let d be a positive integer, and let $q = p^d$. Let α be a primitive element of $\mathbb{F}_q$, and let $M|q-1$. Following the notation from [40], for $0 \leq k \leq M-1$, we set $D_k = \{\alpha^{Mi+k} - 1 | 0 \leq i < (q-1)/M\}$. The M-ary Sidelnikov sequence $\mathbf{s} = s_0 s_1 s_2 \ldots$ is the sequence of period $q-1$ whose first $q-1$ elements are defined as follows: for $0 \leq j < q-1$,

$$s_j = \begin{cases} 0 & \text{if } \alpha^j = -1 \\ k & \text{if } \alpha^j \in D_k \end{cases}.$$

For instance, consider the case in which $p = 17$, $d = 1$, $\alpha = 3$, and $M = 2$. Here, we get that $D_0 = \{0, 1, 3, 7, 8, 12, 14, 15\} = \{0, \alpha^0, \alpha^1, \alpha^{11}, \alpha^{10}, \alpha^{13}, \alpha^9, \alpha^6\}$, $D_1 = \{2, 4, 5, 6, 9, 10, 11, 13\} = \{\alpha^{14}, \alpha^{12}, \alpha^5, \alpha^{15}, \alpha^2, \alpha^3, \alpha^7, \alpha^4\}$, and $\alpha^8 = 16 = -1$. So, in this case, $\mathbf{s} = 0011110100001011...$

The Sidelnikov sequences were originally discovered by Sidelnikov in 1969 [86]. In the binary case (i.e. the case in which $M = 2$) these sequences were rediscovered independently by Lempel, Cohn, and Eastman in 1977 [62]. Consequently, we follow the authors of [59] in referring to the M-ary Sidelnikov sequences as Sidelnikov-Lempel-Cohn-Eastman (SLCE) sequences in the case that $M = 2$.

It is known that the SLCE sequences have three-valued autocorrelation, with out-of-phase autocorrelation values of magnitude at most 4 [62]; we provide Lempel, Cohn, and Eastman's proof of this fact in Chapter 3 of this

thesis (indeed, the fact follows as a direct consequence of Theorem 3.3.1). The M-ary Sidelnikov sequences also have out-of-phase autocorrelation values of magnitude at most 4 in terms of a more general version of the autocorrelation function [86]. Furthermore, it is clear from the definition of the SLCE sequences that they have the balance property (in fact, the M-ary Sidelnikov sequences satisfy a generalized version of the balance property). Consequently, the class of Sidelnikov sequences is one of the best known classes of sequences. So, it is of interest to determine which other properties these sequences posses, in order to determine whether they might be useful for applications.

We conclude this section by presenting an alternative characterization of the SLCE sequences, due to Lempel, Cohn, and Eastman [62], that plays a central role in our work in this thesis. We adopt the following convention.

Notation 2.4.1. *For an integer $i \in \{1, \ldots, p-1\}$, we refer to the corresponding element of $\mathbb{F}_p^*$ by italicizing i.*

Notation 2.4.2. *Let $Y := \{y \in \mathbb{F}_q^* \mid y = x(1-x)$ for some $x \in \mathbb{F}_q^*\}$. Let $S := D_1$ (for the case in which $M = 2$).*

Theorem 2.4.3. $S^c = -4Y$.

Proof. For $\gamma, x \in \mathbb{F}_q^*$,

$$x(1-x) = \gamma \iff (2x-1)^2 = 1 - 4\gamma \iff \gamma = -4^{-1}((2x-1)^2 - 1).$$

If we let x run through the elements of $\mathbb{F}_q^* \setminus \{1\}$, then $-4^{-1}((2x-1)^2-1)$ runs through the elements of $-4^{-1}D_0$ save for 0 (twice) as well as $-4^{-1}(-1) = 4^{-1}$ (once). Hence, $Y = -4^{-1}S^c$, and so $S^c = -4Y$. $\square$

2.4.1 Array structure of the Sidelnikov sequences

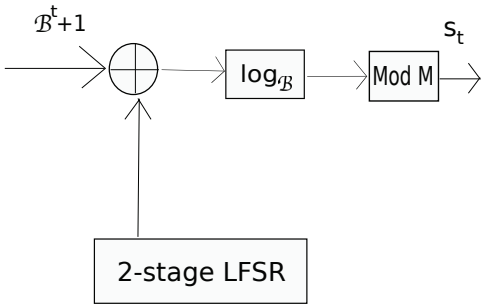
In this section we present some nice structural results due to Gong and Yu [40] that deepen the analogy between the Sidelnikov sequences and the m-sequences. If γ is a generator of the finite field $\mathbb{F}_q$, then for $x \in \mathbb{F}_q^*$, we set $\log_\gamma(x) = i$, where i is the unique integer such that $0 \leq i \leq q-2$ and $\gamma^i = x$. For the remainder of this subsection, let p be an odd prime, let $d = 2m$, for some positive integer m, let $q = p^d$, let α be a primitive element of $\mathbb{F}_q$, let $M | p^m - 1$, and let $\beta = \alpha^{p^m+1}$, so that β is a primitive element of $\mathbb{F}_{p^m}$. The following result from [40] shows how Sidelnikov sequences over $\mathbb{F}_q$ can be determined via computations in the subfield $\mathbb{F}_{p^m}$.

Theorem 2.4.4. *The first period of an M-ary Sidelnikov sequence over $\mathbb{F}_q$ can be represented as follows: for $0 \leq t \leq q-2$,*

$$s_t \equiv log_\beta(\beta^t + Tr_{\mathbb{F}_q/\mathbb{F}_{p^m}}(\alpha^t) + 1) \pmod{M}.$$

This result enables relatively efficient implementation of Sidelnikov sequences over $\mathbb{F}_q$ via circuitry designed for computations in $\mathbb{F}_{p^m}$. Since $\mathbb{F}_q$ is a degree 2 extension of $\mathbb{F}_{p^m}$, it follows that the term $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^m}}(\alpha^t)$ in the above expression is an element of an m-sequence that can be implemented

by a two-stage LFSR. This m-sequence can be summed term-wise modulo p with the sequence of elements of the form $\beta^t + 1$; one can then apply $\log_\beta$ to the resulting sequence and, finally, reduce the sequence so obtained mod M. The following diagram, which is essentially Figure 1 from [40], illustrates this implementation.



Using Theorem 2.4.4, Gong and Yu are able to show that the Sidelnikov sequences have an array structure somewhat similar to the array structure of the m-sequences, at least in the case that q is an even power of an odd prime [40, Theorem 2].

Theorem 2.4.5. *Let* $\mathbf{s}$ *be an M-ary Sidelnikov sequence over* $\mathbb{F}_q$*. Arrange the entries of the first period of* $\mathbf{s}$ *lexicographically into a* $(p^m - 1) \times (p^m + 1)$ *array. Let* v_ℓ *be the* ℓ*-th column of this array, and denote the entry from row*

t, column ℓ as $v_\ell(t)$. If $M = 2$, then $v_0 = \mathbf{0}$ and if $M > 2$, then v_0 is equal to a constant (from $\mathbb{Z}/M\mathbb{Z}$) times the vector whose entries are taken from the first period of a M-ary Sidelnikov sequence over $\mathbb{F}_{p^m}$. For $1 \leq \ell \leq \lfloor \frac{p^m+1}{2} \rfloor$,

$$v_{p^m+1-\ell}(t) = v_\ell(t - \ell + 1).$$

Hence, for $1 \leq \ell \leq \lfloor \frac{p^m+1}{2} \rfloor$, v_ℓ is cyclically equivalent to $v_{p^m+1-\ell}$. Furthermore, the column $v_{\frac{p^m+1}{2}}$ has period dividing $\frac{p^m-1}{2}$.

Consider the following example (which is Example 1 from [40]). Let $p = 7$, $m = 1$, and $M = 6$. Note that one can construct the finite field $\mathbb{F}_{7^2}$ from $\mathbb{F}_7$ using the primitive polynomial $x^2 + x + 3$. We arrange the first period of a 6-ary Sidelnikov srquence of period $7^2 - 1$ into a $(7 - 1) \times (7 + 1)$ array as follows.

$$\begin{pmatrix} 4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\ 2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\ 2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\ 0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\ 4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \end{pmatrix}$$

The first column, v_0, is equal to 2 times the first period of the 6-ary Sidelnikov sequence 241053... of period $7 - 1$. Furthermore, for each t, $v_7(t) = v_1(t)$, $v_6(t) = v_2(t - 1)$, and $v_5(t) = v_3(t - 2)$. Finally, v_4 has period $(7 - 1)/2$.

We conclude by noting that the authors of [57] have obtained further

results concerning the array structure of the Sidelnikov sequences.

2.4.2 Families of Sidelnikov sequences

Several authors have used Sidelnikov sequences to construct families of sequences with low cross-correlation in a manner similar to the way that m-sequences are used to construct the Gold sequences. This technique is sometimes called the "shift and add" method. If $c \in \mathbb{Z}/M\mathbb{Z}$, then we stipulate that $c\mathbf{a}$ is the sequence whose ith entry is ca_i and we say that $c\mathbf{a}$ is a *constant multiple* of $\mathbf{a}$. The authors of [23] consider a family consisting of term-wise sums of constant multiples of a Sidelnikov sequence with constant multiplies of one of its shifts. The authors from [24] enlarge the family from [23] by adding in termwise sums of constant multiples of a Sidelnikov sequence with constant multiples of its decimation by -1.

The authors of [23] and [24] have given upper bounds on the cross-correlation of the sequences from their Sidelnikov families. It is convenient for us to quote the result from [24] since we will make use of it later.

Theorem 2.4.6. *Let q be a prime power, and let $\mathbf{s}$ be an M-ary Sidelnikov sequence over $\mathbb{F}_q$. Let $\mathcal{F}$ be the family consisting of all termwise sums of constant multiples of $\mathbf{s}$ and its decimation by -1. Then the maximum cross-correlation of two sequences from $\mathcal{F}$ is less than or equal to $4\sqrt{q} + 5$.*

Finally, we note that the authors of [40] have obtained large families of sequences with good cross-correlation properties by combining the families

from [23] with sequences obtained from the columns of the array representations of the Sidelnikov sequences described in the previous section.

2.4.3 Research

The practical applications mentioned earlier in this chapter have motivated a significant amount of research into finding sequences with good properties and determining the properties of known classes of sequences. Thus, they have given rise to a new branch of theoretical (but potentially applicable) mathematics: the study of the pseudo-randomness properties of sequences with elements from finite rings. There are essentially two general problems considered by researchers in this field: the problem of finding new sequences with good properties, and the problem of determining the properties of promising known classes of sequences. The theoretical business of answering these questions is different than the practical matter of deciding which sequence will work best for a given application. But, of course, the hope of any researcher in this field is that their work might wind up being useful.

Since the SLCE sequences are known to be balanced sequences with nearly ideal autocorrelation, there is sufficient motivation to try to determine what other properties they might have. In this thesis, we consider two open problems concerning these sequences.

Firstly, we attempt to determine which decimations of the SLCE sequences give rise to shift-inequivalent sequences. Thus, we attempt to find

an analogue of Theorem 2.3.6 for SLCE sequences. This problem was originally considered by Lempel, Cohn, and Eastman [62]. They mention that it "appears to be a hard problem" [62]. Indeed, very little progress has been made in this direction since the work of Lempel, Cohn, and Eastman. The authors of [6] also mention this problem as being open.

Secondly, we attempt to determine the linear complexity of the SLCE sequences. Unlike the m-sequences, the SLCE sequences are not defined in terms of their minimal polynomials. So, it is not a trivial matter to solve this problem. Indeed, due to certain technical considerations, this problem is, in fact, quite hard. Despite the efforts of a number of authors over the past fifteen years, it is still unsolved (see [49], [59], and [73]).

We make significant progress towards solving both of these problems (although we are unable to completely solve either of them). Our results towards determining the shift-inequivalent decimations of the SLCE sequences are presented in Chapter 5, and our results towards determining the linear complexity of the SLCE sequences are presented in Chapter 6. There are many open questions concerning the SLCE (and, more generally, the Sidelnikov) sequences. We identify a number of these problems in Chapter 7.

In the next two chapters, we develop the theoretical framework used in our study of the SLCE sequences. In Chapter 3, we introduce difference sets and almost difference sets (which are combinatorial objects that are closely related to the sequences discussed in this chaper), and we also introduce some of the tools that are used to study these combinatorial objects, such as group

rings and characters. In Chapter 4 we introduce Gauss and Jacobi sums, and we prove our formula for the character values of the almost difference sets associated with the SLCE sequences.

Chapter 3

Group rings and difference sets

In this chapter, we introduce combinatorial objects called difference sets (and almost difference sets). As we will see, the existence of one of these objects is equivalent to the existence of a periodic binary sequence with certain pseudo-randomness properties. Indeed, the combinatorial language of the theory of difference sets provides a convenient view point from which to study the pseudo-randomness properties of periodic binary sequences.

The existence of a difference set (or almost difference set) is equivalent to the existence of a group ring element satisfying certain equations. By applying characters to such a group ring element, one can deduce that the existence of a difference set (or almost difference set) implies the existence of elements in certain cyclotomic fields satisfying certain special equations. Thus, tools from algebraic number theory can be brought to bear on existence (and structural) questions concerning difference sets (and almost difference

sets).

In this chapter and the next, we review all of the facts from algebraic number theory that we make use of later in this thesis. We conclude this chapter by explaining how group characters and facts about cyclotomic fields can be used to gain insight into problems of the type with which we are concerned: namely, determining the linear complexity of a periodic binary sequence and determining which decimations of that sequence give rise to shift-inequivalent sequences.

3.1 Difference sets

Let v, k, and λ be positive integers. Let $(G, +)$ be a (finite) group of order v. A subset $D \subseteq G$ of size k is called a (v, k, λ) *difference set* if for every $g \in G \setminus \{0\}$, there exist exactly λ pairs $d_i, d_j \in D$ such that $d_i - d_j = g$. We shall be most interested in the case in which G is a cyclic group. In this case, we generally just consider G to be $\mathbb{Z}/v\mathbb{Z}$ (so that D is a subset of the residues mod v). When G is cyclic, D is called a *cyclic difference set*.

Example 3.1.1. *Let $v = 7$, $k = 4$, and $\lambda = 2$. The subset $\{0, 3, 5, 6\}$ of $\mathbb{Z}/7\mathbb{Z}$ is a (v, k, λ) cyclic difference set.*

We note three simple facts about cyclic difference sets. There are analogues of these facts that hold for difference sets more generally, but we shall not need them. It is particularly simple to justify all of these facts using the group ring structure that we introduce in Section 3.3.

Let $D \subseteq \mathbb{Z}/v\mathbb{Z}$ be a (v, k, λ) cyclic difference set.

• For each $x \in \mathbb{Z}/v\mathbb{Z}$, $x + D$ is also a (v, k, λ) cyclic difference set. The sets of the form $x + D$ are called *shifts* of D.

• For each $t \in (\mathbb{Z}/v\mathbb{Z})^*$, tD is also a (v, k, λ) cyclic difference set. The sets of the form tD (for $t \in (\mathbb{Z}/v\mathbb{Z})^*$) are called *multiples* of D.

• The set complement D^c of D in $\mathbb{Z}/v\mathbb{Z}$ is a $(v, v - k, v - k - \lambda)$ cyclic difference set.

There is a simple connection between cyclic difference sets and periodic binary sequences.

Notation 3.1.2. *Let v be a positive integer, and let $A \subseteq \mathbb{Z}/v\mathbb{Z}$. The periodic binary sequence corresponding to A is the sequence $\mathbf{a} = a_0a_1a_2...$ of period v whose first v elements are defined by the rule that for $i' \in \{0, ..., v - 1\}$, $a_{i'} = 1$ if $i \in A$ and $a_{i'} = 0$ otherwise.*

Suppose $D \subseteq \mathbb{Z}/v\mathbb{Z}$ is a (v, k, λ) cyclic difference set. Let $\mathbf{d}$ be the periodic binary sequence corresponding to D. It is not hard to show that $\mathbf{d}$ has two-valued autocorrelation

$$\mathcal{C}_{\mathbf{d},\mathbf{d}}(\tau) = \begin{cases} v - 4(k - \lambda) & \text{if } \tau \neq 0, \\ v & \text{if } \tau = 0. \end{cases}$$

Conversely, given a periodic binary sequence with two-valued autocorrelation, one can easily obtain a cyclic difference set (see [39, Section 7.1.2] for proofs of both these claims).

Example 3.1.3. *Using the* $(7, 4, 2)$ *cyclic difference set* $\{0, 3, 5, 6\}$ *from Example 3.1.1, we obtain the sequence* 1001011... *from Example 2.1.1. We have already seen that this sequence has two-valued autocorrelation.*

We are particularly interested in cyclic difference sets that give rise to periodic sequences with good randomness properties. Let t be a positive integer. Let $v = 4t - 1$, $k = 2t - 1$, and $\lambda = t - 1$. Suppose D is a (v, k, λ) cyclic difference set. Then the periodic binary sequence $\mathbf{d}$ associated with D is (clearly) balanced and has out of phase autocorrelation $v - 4(k - \lambda) = -1$. Hence, $\mathbf{d}$ has properties R-1 and R-3.

Difference sets with parameters $v = 4t - 1$, $k = 2t - 1$, and $\lambda = t - 1$ are called *Hadamard difference sets*. The name is due to the fact that these difference sets can be used to construct other useful combinatorial objects called Hadamard matrices (see [39, Section 7.1.2 and Section 2.5]). For a discussion of Hadamard matrices, see [51].

Example 3.1.4. *Let* $v = 7 = 4 \times 2 - 1$, $k = 3 = 2 \times 2 - 1$, *and* $\lambda = 1 = 2 - 1$. *Then* $\{1, 2, 4\} \subseteq \mathbb{Z}/7\mathbb{Z}$ *is a* (v, k, λ) *cyclic Hadamard difference set.*

In the next two subsections, we will discuss some of the known constructions of cyclic Hadamard difference sets.

3.1.1 Cyclotomic difference sets

Let p be an odd prime, let $q = p^d$ (for some positive integer d) and let $e|q-1$ (so that $q = ef + 1$, for some positive integer f). Let α be a generator of

$\mathbb{F}_q^*$. Then the eth cyclotomic classes are the sets C_i defined as follows: for $i = 0, ..., e-1$, $C_i := \{\alpha^{es+i} : s = 0, 1, ..., f-1\}$. For instance, if $q = p$ (i.e. if q is prime) and $e = 2$, then C_0 is the set of quadratic residues mod p and C_1 is the set of quadratic non-residues mod p.

Several authors have used cyclotomic classes (and unions of cyclotomic classes) to construct difference sets in the *additive* groups of finite fields. Note that such difference sets are cyclic exactly when the finite fields in question have prime order.

The earliest result of this type is due to Paley [77].

Theorem 3.1.5. *Let p be a prime equivalent to 3 mod 4. Let C_0 and C_1 be the 2nd cyclotomic classes in $\mathbb{F}_p^*$ (so that C_0 is the set of quadratic residues mod p). Then C_0 is a cyclic Hadamard difference set in $(\mathbb{F}_p.+)$.*

For example, $\{1, 3, 4, 5, 9\} \subseteq \mathbb{F}_{11}$ is a $(11, 5, 2)$ cyclic Hadamard difference set.

It is natural to ask for which p and e the cyclotomic class C_0 winds up being a cyclic difference set. The answer to this question can be given in terms of mathematical objects called cyclotomic numbers. These objects were first defined and used by Gauss in his celebrated work on the problem of constructing regular polygons using only a straight edge and compass (see, for instance, [88, Section 1.1]).

Let q be an odd prime power, and let $e|(q-1)$. For fixed $i, j \in \{0, 1, ..., e-1\}$, we stipulate that the *cyclotomic number* (i, j) is the number of solutions

of the equation

$$z_i + 1 = z_j,\ z_i \in C_i,\ z_j \in C_j.$$

Thus, the cyclotomic numbers encode nontrivial information: insight into the connection between the multplicative and additive structures of $\mathbb{F}_q$.

In the 1950s, Emma Lehmer showed how cyclotomic numbers can be used to decide whether or not C_0 is a difference set (for a given p and e) [63].

Theorem 3.1.6. *Let p be an odd prime, and let $e|(p-1)$. C_0 is a difference set in $\mathbb{F}_p$ if and only if $(i,0) = (f-1)/e$ for $i = 0, 1, ..., e-1$.*

So long as one can evaluate the cyclotomic numbers $(i,0)$, one can use Theorem 3.1.6 to decide whether (for a given p and e) C_0 is a difference set in $\mathbb{F}_p$. It can be shown that for an odd prime p, C_0 can only be a difference set in $\mathbb{F}_p$ when e is even and $p = ef + 1$, for some odd number f [88], so we consider what is known about cyclotomic numbers for even numbers e.

In the case that $e = 2$, the formulae for the cyclotomic numbers are quite simple . Indeed, this case was first considered in Gauss's work on constructing regular polygons (see [88, Lemma 2.6]).

Theorem 3.1.7. *Let q be an odd prime power, let $e = 2$, and let $q = 2f + 1$. Then the cyclotomic numbers are given as follows. If f is even, then $(0,0) = (f-2)/2$, and $(0,1) = (1,0) = (1,1) = f/2$. If f is odd, then $(0,0) = (1,0) = (1,1) = (f-1)/2$, and $(0,1) = (f+2)/2$.*

It is a simple matter to use Theorem 3.1.7 in conjunction with Lehmer's

criterion (Theorem 3.1.6) to recover Paley's result on quadratic residue difference sets (Theorem 3.1.5).

For larger values of e, the formulae expressing the cyclotomic numbers are more complicated. As an example, we present the formulae for the case in which $e = 4$ and f is odd. Firstly, we note that it can be shown by elementary techniques that in this case, the cyclotomic numbers take on five different values, which we shall denote A, B, C, D, and E. Furthermore, one can show that the cyclotomic numbers take on these values according to the dictates of the following table, wherein the entry in row i, column j is the cyclotomic number (i, j).

$$\begin{array}{cccc} A & B & C & D \\ E & E & D & B \\ A & E & A & E \\ E & D & B & E \end{array}$$

For proofs of these claims, see [88, Section 2.1].

It is known that for a prime power $q \equiv 1 \pmod 4$, there exists a unique integer s and an integer t (unique up to sign) such that $q = s^2 + 4t^2$, $\gcd(s, q) = 1$, and $s \equiv 1 \pmod 4$ [65, Section 7.2]. We say that $q = s^2 + 4t^2$ is the *proper representation* of q. The following result was originally proven by Gauss using elementary techniques [33] but has since been re-proven using more modern methods (see, for example, [88, Lemma 19]).

Lemma 3.1.8. *Let q be an odd prime power congruent to 1 mod 4, and let*

$q = s^2 + 4t^2$ be its proper representation. Let $e = 4$. Assume that $q = ef + 1$, for some odd number f. Then the numbers A, B, C, D, and E from the above array satisfy the following relations: $16A = q - 7 + 2s$, $16B = q + 1 + 2s - 8t$, $16C = q + 1 - 6s$, $16D = q + 1 + 2s + 8t$, *and* $16E = q - 3 - 2s$.

Using Lemma 3.1.8 in conjunction with Theorem 3.1.6, it is easy to deduce the following result, which was originally proven by Chowla using different techniques [22].

Theorem 3.1.9. *If $p \equiv 1 \pmod 4$ and $e = 4$, then C_0 forms a difference set in $\mathbb{F}_p$ if and only if there exists an integer t such that $p = 1 + 4t^2$.*

As e gets larger, the formulae for the cyclotomic numbers become increasingly more complicated, to the extent that for large values of e, it is generally deemed infeasible to explicitly derive expressions for these numbers (see, for instance, the comment on p.2 of [76]). However, explicit evaluations are known for values of e less than or equal to 24 [11, p.99]. In terms of difference sets, cyclotomic numbers have been employed to show that when $e = 8$, C_0 is sometimes a difference set but that for many other values of e, C_0 is never a difference set (see [88, Part I]).

Now, C_0 can only be a Hadamard difference set when $e = 2$. However, it is possible to construct Hadamard difference sets by taking unions of cyclotomic classes. Marshall Hall discovered Hadamard difference sets of this type in the case that $e = 6$ [44]. Hall's work also relies on cyclotomic numbers.

It turns out that cyclotomic numbers are closely related to certain types

of character sums called Gauss and Jacobi sums [11, Theorems 2.5.1 and 2.1.3]. Because of the difficulty of working directly with cyclotomic numbers for large values of e, some authors have elected to study difference sets using character sums instead (see, for example, the comment on p. 246 of [30]). For instance, in [30], Feng and Xiang use Gauss sums to prove the validity of a construction of (non-cyclic) difference sets in the additive groups of certain finite fields formed by taking unions of cyclotomic classes.

We take an analogous approach in this thesis. Cyclotomic numbers have proven to be useful tools for studying the SLCE sequences. Indeed, we summarize some of the results obtained using cyclotomic numbers in Chapter 6. However, we have elected to study the SLCE sequences using Jacobi sums.

We conclude by mentioning that it is possible to extend the approach outlined in this section from prime fields to rings of the form $\mathbb{Z}_{pr}$, where p and r are primes. Whiteman was able to show that these rings have a multiplicative structure somewhat analogous to that of finite fields. Furthermore, he defined versions of cyclotomic classes and cyclotomic numbers in these rings. Whiteman was able to use his theoretical framework to prove the existence of cyclic Hadamard difference sets in rings of the form $\mathbb{Z}_{p(p+2)}$, where p and $p+2$ are both primes [95]. For a thorough discussion of Whiteman's results, as well as an exploration of various generalizations, see [88].

3.1.2 Constructing difference sets using projective geometry

In this section, we present some constructions of cyclic Hadamard difference sets using tools from projective geometry. But before presenting the constructions themselves, we begin by recalling some relevant facts about projective geometry.

Background from projective geometry

In the 17th century, Johannes Kepler and Gérard Desargues independently had the insight that the process of solving certain problems in Euclidean incidence geometry could be facilitated by the introduction of new mathematical objects called points at infinity. To each set of parallel lines in the Euclidean plane, they associate a new point (a *point at infinity*) and stipulate that this point lies on each line in the set (and on no other lines). They also stipulate the existence of an additional line, called a *line at infinity*. The line at infinity passes through all of the points at infinity, but not through any other points. Thus, in the extended Euclidean plane, every pair of lines intersect one another in exactly one point.

The extended Euclidean plane is an example (indeed, the prototypical example) of a type of incidence structure called a projective geometry. For a statement of the axioms of projective geometry, see [14, Section 1.2]. A *Desarguesian* projective geometry is a projective geometry in which the The-

orem of Desargues is true (see, for instance, [20, Section 2.3] for a statement of Desargues' Theorem). The Theorem of Desargues is true in the extended Euclidean plane. So, Desarguesian projective geometries have more in common with the extended Euclidean plane than do projective geometries in general.

We mention that projective geometries need not have infinitely many points (see, for instance, [14, p.89, Exercise 5]). Indeed, in this thesis, we will only be interested in finite, Desarguesian projective geometries. It turns out that one can construct such structures using ideas similar to the ideas used to coordinatize the extended Euclidean plane with homogeneous coordinates (see [20, Sections 12.1-12.3]).

Let q be a prime power, and let $d \geq 2$ be a positive integer. Let $\mathbb{F}_q^{d+1}$ denote the vector space of all $(d+1)$-tuples of elements from $\mathbb{F}_q$. Define an incidence structure $\mathrm{PG}(d, \mathbb{F}_q)$ on the subspaces of $\mathbb{F}_q^{d+1}$ as follows. Call the one dimensional subspaces *points*, the two-dimensional subspaces *lines*, and the three dimensional subspaces *planes*. In general, call the k-dimensional subspaces of $\mathbb{F}_q^{d+1}$ $(k-1)$-*dimensional subspaces* of $\mathrm{PG}(d, \mathbb{F}_q)$. Finally, call the d-dimensional subspaces of $\mathbb{F}_q^{d+1}$ *hyperplanes* of $\mathrm{PG}(d, \mathbb{F}_q)$. Incidence amongst the objects in $\mathrm{PG}(d, \mathbb{F}_q)$ is inherited from set-theoretical containment in $\mathbb{F}_q^{d+1}$. The points and lines of $\mathrm{PG}(d, \mathbb{F}_q)$ form a Desarguesian projective geometry.

Let $v = (q^{d+1} - 1)/(q - 1)$, and let $k = (q^d - 1)/(q - 1)$. It is easy to show that $\mathrm{PG}(d, \mathbb{F}_q)$ contains v points and that each hyperplane of $\mathrm{PG}(d, \mathbb{F}_q)$ contains k points [14, Theorem 1.5.3].

Finally, we note that one of the original applications of projective geometry was proving incidence results pertaining to conics in the Euclidean plane (see, for example, Pascal's Theorem [20, Theorem 9.23]). Now, an *oval* in a projective geometry is a set of points, no three of which are collinear, and each of which lies on exactly one tangent. All of the conics are ovals.

In the sequel, we shall be interested in a slight relaxation of the concept of an oval. A *hyperoval* in a projective geometry is a set of points, no three of which are collinear.

The constructions

Recall that the additive group of $\mathbb{F}_{q^{d+1}}$ is isomorphic to $\mathbb{F}_q^{d+1}$. Hence, we can impose a multiplicative structure on $\mathbb{F}_q^{d+1}$ by identifying each $(d+1)$-tuple in $\mathbb{F}_q^{d+1}$ with an element of $\mathbb{F}_{q^{d+1}}$. For each $\beta \in \mathbb{F}_{q^{d+1}}^*$, let $[\beta]$ denote the point of $\mathrm{PG}(d, \mathbb{F}_q)$ containing the $(d+1)$-tuple associated with β.

Let α be a generator of $\mathbb{F}_{q^{d+1}}^*$. Singer proved that the points $[1]$, $[\alpha]$, $[\alpha^2]$, ..., $[\alpha^{v-1}]$ are all distinct. Hence, since $\mathrm{PG}(d, \mathbb{F}_q)$ contains only v points, it follows that one can impose a cyclic group structure on the points of $\mathrm{PG}(d, \mathbb{F}_q)$. Indeed, we write $G = \langle [\alpha] \rangle$ to denote the group of points of $\mathrm{PG}(d, \mathbb{F}_q)$.

Let $\lambda = (q^{d-1}-1)/(q-1)$. The following important result is due to Singer [87].

Theorem 3.1.10. *Let H be the set of points in G contained in some hyperplane of $PG(d, \mathbb{F}_q)$. Then H is a (v, k, λ) cyclic difference set.*

In the special case that $q = 2$, H is a cyclic difference set with parameters $(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1)$. So, in this case, H is a cyclic Hadamard difference set.

For each $\beta \in \mathbb{F}^*_{q^{d+1}}$, $\mathrm{Tr}_{\mathbb{F}_{q^{d+1}}/\mathbb{F}_q}(\beta x)$ is a linear transformation from $\mathbb{F}_{q^{d+1}}$ onto $\mathbb{F}_q$. Hence, by the Dimension Theorem, the nullity of this map is d. In other words, $\mathrm{Ker}\left(\mathrm{Tr}_{\mathbb{F}_{q^{d+1}}/\mathbb{F}_q}(\beta x)\right)$ is a hyperplane in $\mathrm{PG}(d, \mathbb{F}_q)$. Furthermore, it is straightforward to show that every hyperplane can be obtained as the kernel of such a map [8, p. 103].

Thus, we have a method for generating Singer difference sets. For each $\beta \in \mathbb{F}^*_{q^{d+1}}$, the set

$$H_\beta = \{[\gamma] \in G : \mathrm{Tr}_{\mathbb{F}_{q^{d+1}}/\mathbb{F}_q}(\beta\gamma) = 0\} \tag{3.1.1}$$

is a Singer difference set.

In the special case that $q = 2$, it is clear that $G \cong \mathbb{F}^*_{2^{d+1}}$. Also, in this case, each one-dimensional subspace of $\mathbb{F}_2^{d+1}$ contains only one nonzero element. So, we can identify the points of $\mathrm{PG}(d, \mathbb{F}_2)$ with the elements of $\mathbb{F}^*_{2^{d+1}}$. Note that the Singer difference sets in G can be generated as follows: for each $\beta \in \mathbb{F}^*_{2^{d+1}}$, simply set $H_\beta = \{\gamma \in \mathbb{F}^*_{2^{d+1}} : \mathrm{Tr}_{\mathbb{F}_{2^{d+1}}/\mathbb{F}_2}(\beta\gamma) = 0\}$.

For example, let α be a root of the irreducible polynomial $x^3 + x + 1$ over $\mathbb{F}_2$. Then $H_1 = \{\alpha, \alpha^2, \alpha^4\}$. In residue ring notation, H_1 is the difference set $\{1, 2, 4\}$ in $\mathbb{Z}/7\mathbb{Z}$. Note that H_1 is the complement of the difference set from Example 3.1.1. Indeed, it is clear from their respective definitions that for

$q = 2$, the Singer difference sets are the complements of the difference sets associated with the m-sequences.

We note also that the Singer difference sets have an array structure similar to the array structure of the m-sequences outlined in Section 2.4.1 (see, for instance, [8, Section V.A]). By exploiting this array structure, Gordon, Mills, and Welch were able to use the Singer difference sets to construct another important family of difference sets, which are now known as the Gordon-Mills-Welch (or, GMW) difference sets [41]. However, we will not explore their construction in this thesis.

We conclude this section by outlining a recent geometric construction of $(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1)$ cyclic Hadamard difference sets that are fundamentally different from the Singer difference sets (in the sense that the decimations of the sequences associated with these difference sets are shift-inequivalent to the m-sequences associated with the Singer difference sets). This construction is due to Maschietti [70]. Our outline essentially follows the discussion given in [12, Section VI.17].

A *permutation polynomial* on a finite field $\mathbb{F}_q$ is a polynomial with coefficients from $\mathbb{F}_q$ that induces a bijection from $\mathbb{F}_q$ to itself. For instance, let α be a root of the polynomial $x^2 + x + 1$ (which is irreducible over $\mathbb{F}_2$). Then $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2\}$. Let $f(x) = x^2$. It is easily verified that $f(x)$ is a permutation polynomial on $\mathbb{F}_{2^2}$.

For a polynomial $f(x)$ on $\mathbb{F}_{2^{d+1}}$, define the set $H(f)$ as follows:

$$H(f) = \{(1, x, f(x)) : x \in \mathbb{F}_{2^d}\} \cup \{(0, 1, 0), (0, 0, 1)\}. \tag{3.1.2}$$

Segre proved that if $f(x)$ is a permutation polynomial on $\mathbb{F}_{2^{d+1}}$ of degree at most $2^{d+1}-2$ with $f(0) = 0$ and $f(1) = 1$ such that the map f_s defined by the rules that $f_s(0) = 0$ and for $x \neq 0$, $f(x) = \frac{f(x+s)+f(s)}{x}$ is also a permutation polynomial on $\mathbb{F}_{2^{d+1}}$ for each $s \in \mathbb{F}_{2^{d+1}}$, then the set $H(f)$ is a hyperoval in $\mathrm{PG}(2, \mathbb{F}_{2^{d+1}})$. Segre also established that every hyperoval in $\mathrm{PG}(2, \mathbb{F}_{2^{d+1}})$ is essentially the same as a hyperoval of this form (see [50, Theorem 8.4.2] for a proof of Segre's result).

As an example, we can make use of the permutation polynomial mentioned above to construct the following hyperoval in $\mathrm{PG}(2, \mathbb{F}_{2^2})$:

$$H(f) = \{(1, 0, 0), (1, 1, 1), (1, \alpha, \alpha^2), (1, \alpha^2, \alpha)\} \cup \{(0, 1, 0), (0, 0, 1)\}.$$

Indeed, this is Example 9.4 from [39].

If, as in our example, the permutation polynomial is a monomial (say $f(x) = x^k$) then we say that $H(f)$ is a *monomial hyperoval*. The following list comprises all known monomial hyperovals in $\mathrm{PG}(2, \mathbb{F}_{2^d})$. In fact, Glynn has conjectured that there are no others [35].

• The *translation hyperovals*, which have the form $H(x^{2^n})$, where $\gcd(n, d) = 1$. These objects were discovered independently by Segre and Bartocci [7] and Payne [78].

• The *Segre* hyperovals, which have the form $H(x^6)$, for odd $d \geq 5$. These objects were discovered by Segre and Bartocci [7].

• The *Glynn* hyperovals, which have the form $H(x^{\sigma+\gamma})$ and $H(x^{3\sigma+\gamma})$ for odd $d \geq 7$. Here, we have that $\sigma = 2^{(d+1)/2}$; for $d = 4m-1$, $\gamma = 2^m$, and for $d = 4m+1$, $\gamma = 2^{3m+1}$.

For a given positive integer k, let $\tau : \mathbb{F}_{2^{d+1}} \to \mathbb{F}_{2^{d+1}}$ be the map defined by the rule $\tau(x) = x^k + x$. Let $D(x^k)$ be the set defined as follows:

$$D(x^k) = \tau(\mathbb{F}_{2^{d+1}}) \setminus \{0\}. \tag{3.1.3}$$

The following important result is due to Maschietti [70].

Theorem 3.1.11. *Let k and d be positive integers. The set $H(x^k)$ is a hyperoval in $PG(2, \mathbb{F}_{2^{d+1}})$ if and only if the set $D(x^k)$ is a $(2^{d+1}-1, 2^d - 1, 2^{d-1}-1)$ cyclic difference set in $\mathbb{F}^*_{2^{d+1}}$.*

Maschitetti also proved that $H(x^k)$ is a translation hyperoval if and only if $D(x^k)$ is a Singer difference set [70]. However, Evans et al were able to show that for large enough values of d, the cyclic difference sets corresponding to Segre and Glynn hyperovals arising from Theorem 3.1.11 are essentially different from all other known cyclic diffference sets having the same parameters [29].

3.2 Almost difference sets

As we mentioned in Section 2.1.4, one can relax Randomness Postulate R-3 somewhat without significant cryptographic consequences. Cyclic difference sets have been shown to correspond to periodic binary sequences with two-valued autocorrelation. Many authors have been led to consider combinatorial objects corresponding to periodic binary sequences with three-valued autocorrelation. There are several generalizations of difference sets that have been considered in the literature, two of the most prominent being partial difference sets and relative difference sets. For a discussion of partial difference sets, see [67]. For a discussion of relative difference sets, see [12, Section VI.10]. In this section, we discuss a different generalization, which is more relevant for our purposes.

Let v, k, λ, and r be positive integers. Let $(G, +)$ be a (finite) group of order v. A subset $D \subseteq G$ of size k is called a (v, k, λ, r) *almost difference set* if there exists a set $R \subseteq G \setminus \{0\}$ of size r such that for each $g \in R$, there exist exactly λ pairs $d_i, d_j \in D$ such that $d_i - d_j = g$, and for each $g \in (G \setminus \{0\}) \setminus R$, there exist exactly $\lambda + 1$ pairs $d_i, d_j \in D$ such that $d_i - d_j = g$. Note that in the case that $r = v - 1$ (so that $R = G \setminus \{0\}$) a (v, k, λ, r) almost difference set is just a (v, k, λ) difference set. We shall be most interested in the case in which G is a cyclic group. In this case, we generally just consider G to be $\mathbb{Z}/v\mathbb{Z}$ (so that D is a subset of the residues mod v). When G is cyclic, D is called a *cyclic almost difference set*.

Example 3.2.1. *Let* $v = 13$, $k = 6$, $\lambda = 2$, *and* $r = 6$. *The subset* $D = \{1, 3, 4, 9, 10, 12\}$ *of* $\mathbb{Z}/13\mathbb{Z}$ *is a* (v, k, λ, r) *cyclic almost difference set. Here* $R = \{1, 3, 4, 9, 10, 12\}$. *So,* $R = D$ *in this case. This phenomenon is not characteristic of almost difference sets. However,* D *is also a partial difference set.*

We note that shifts, multiples, and complements of cyclic almost difference sets are also cyclic almost difference sets.

Suppose $D \subseteq \mathbb{Z}/v\mathbb{Z}$ is a (v, k, λ, r) cyclic almost difference set. Let $\mathbf{d}$ be the periodic binary sequence corresponding to D. It is not hard to show that $\mathbf{d}$ has three-valued autocorrelation

$$\mathcal{C}_{\mathbf{e},\mathbf{e}}(\tau) = \begin{cases} v - 4(k - \lambda) & \text{if } \tau \in R, \\ v - 4(k - \lambda - 1) & \text{if } \tau \in \mathbb{Z}/v\mathbb{Z} - \{R \cup \{0\}\}, \\ v & \text{if } \tau = 0. \end{cases}$$

Conversely, given a periodic binary sequence with three-valued autocorrelation, one can easily obtain a cyclic almost difference set [6].

Example 3.2.2. *Using the* $(13, 6, 2, 6)$ *cyclic almost difference set* $\{1, 3, 4, 9, 10, 12\}$ *from Example 3.2.1, we obtain the sequence* 0101100001101..., *which has three-valued autocorrelation.*

We are particularly interested in cyclic almost difference sets that correspond to balanced sequences. These cyclic almost difference sets are the

natural analogues of the cyclic Hadamard difference sets. Several such families of almost difference sets can be constructed using cyclotomic classes. Many of these constructions are due in part to the work of Cunsheng Ding. However, the most basic construction of this type is given by the following theorem, which is due to Paley [77] (and was known prior to the formalization of the concept of an almost difference set); see [6] for a discussion of the methods one could use to prove this result.

Theorem 3.2.3. *Let p be a prime equivalent to 1 mod 4. Let C_0 and C_1 be the 2nd cyclotomic classes in $\mathbb{F}_p^*$ (so that C_0 is the set of quadratic residues mod p). Then C_0 is a cyclic almost difference set in $(\mathbb{F}_p.+)$.*

The almost difference set from Example 3.2.2 can be generated using the construction given in Theorem 3.2.3. For an overview of several other cyclotomic (and generalized cyclotomic) constructions of cyclic almost difference sets, see [6].

Let p be an odd prime, let d be a positive integer, and let $q = p^d$. Let $\mathbf{s}$ be an SLCE sequence defined over $\mathbb{F}_q^*$. Then, as we mentioned in Section 2.4, $\mathbf{s}$ has a three-valued autocorrelation function. Indeed, we will prove this fact in the next section by showing that the set $S \subseteq \mathbb{F}_q^*$ defined in Section 2.4 is a cyclic almost difference set.

3.3 Group rings and characters

We now introduce another way of thinking about sequences and difference sets. Let G be a finite cyclic group of order v with its operation written multiplicatively. The integral group ring $\mathbb{Z}[G]$ consists of all formal sums $\sum_{g\in G} a_g g$, where $a_g \in \mathbb{Z}$ and with addition and multiplication defined as follows:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

and

$$\Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{h\in G} b_h h\Big) = \sum_{f\in G} \Big(\sum_{gh=f} a_g b_h\Big) f.$$

For any subset $A \subseteq G$, we identify A with the group ring sum of all the elements in A; indeed, we refer to this sum as A. More generally, if B is a multiset consisting of the elements $g_1, ..., g_k$ of G and for each $i = 1, ..., k$, the element g_i appears in B b_i times, we associate B with the group ring element $\sum b_i g_i$.

Let $t \in (\mathbb{Z}/v\mathbb{Z})^*$, let $A = \sum a_g g$ be a group ring element, and let $A^{(t)} := \sum a_g g^{t'}$. It is easy to see that $D \subseteq G$ is a (v, k, λ) cyclic difference set in G if and only if D satisfies the group ring equation

$$DD^{(-1)} = (k - \lambda) + \lambda G. \tag{3.3.1}$$

Similarly, it is easy to see the $E \subseteq G$ is a (v, k, λ, r) cyclic almost difference set if and only if there exists a set $R \subseteq G \setminus \{1\}$ of size r for which E satisfies the group ring equation

$$EE^{(-1)} = k + \lambda R + (\lambda + 1)((G \setminus \{1\}) \setminus R). \tag{3.3.2}$$

As a first application of the group ring machinery, we will prove that the set $S \subseteq \mathbb{F}_q^*$ defined in Section 2.4 is a cyclic almost difference set. Indeed, the following result implies that the SLCE sequences have three valued autocorrelation of magnitude at most 4. The proof we give is due to Lempel, Cohn, and Eastman [62].

Theorem 3.3.1. *Let p be an odd prime, let d be a positive integer, and let $q = p^d$. The set $S \subseteq \mathbb{F}_q^*$ is a cyclic almost difference set. Indeed, let $k = (q-1)/2$. If k is odd, then there is a set $R \subseteq \mathbb{F}_q^* \setminus \{1\}$ such that*

$$SS^{(-1)} = k + \frac{k-1}{2}R + \frac{k+1}{2}((\mathbb{F}_q^* \setminus \{1\}) \setminus R).$$

If k is even, then there is a set $R \subseteq \mathbb{F}_q^* \setminus \{1\}$ such that

$$SS^{(-1)} = k + \frac{k-2}{2}R + \frac{k}{2}((\mathbb{F}_q^* \setminus \{1\}) \setminus R).$$

Proof. Let

$$SS^{(-1)} = \sum_{g \in \mathbb{F}_q^*} a_g g.$$

Recall the set D_0 defined in Section 2.4. Let

$$D_0 S^{(-1)} = \sum_{g \in \mathbb{F}_q^*} b_g g,$$

and let

$$-1\, S^{(-1)} = \sum_{g \in \mathbb{F}_q^*} c_g g.$$

Now, $-1+S+D_0 = \mathbb{F}_q^*$, and $\mathbb{F}_q^* S^{(-1)} = k\mathbb{F}_q^*$. So, for each $g \in \mathbb{F}_q^*$, $c_g + a_g + b_g = k$, i.e.

$$a_g + b_g = k - c_g. \tag{3.3.3}$$

Let α be a primitive root of $\mathbb{F}_q^*$, and for $1 \leq i, j \leq k-1$, let $d_i := \alpha^{2i+1} - 1$ and $e_j := \alpha^{2j} - 1$. Note that for each $1 \leq i, j \leq k-1$,

$$1 - \frac{\alpha^{2i+1} - 1}{\alpha^{2j+1} - 1} = \frac{\alpha^{2j+1} - \alpha^{2i+1}}{\alpha^{2j+1} - 1} \frac{\alpha^{-(2j+1)}}{\alpha^{-(2j+1)}} = \frac{\alpha^{2(i-j)} - 1}{\alpha^{2(k-1-j)+1} - 1}.$$

Consequently, for $i \neq j$, $1 - d_i d_j^{-1} = e_{i-j} d_{k-1-j}^{-1}$. So, we deduce that for $g \neq 1$,

$$a_g = b_{1-g}. \tag{3.3.4}$$

Let $g \neq 1$. Applying equations (3.3.3) and (3.3.4) to the elements g, g^{-1}, and $(1-g)^{-1}$, we obtain the following equations:

$$a_g + a_{1-g} = k - c_g, \tag{3.3.5}$$

$$a_{g^{-1}} + a_{1-g^{-1}} = k - c_{g^{-1}}, \tag{3.3.6}$$

and

$$a_{(1-g)^{-1}} + a_{1-(1-g)^{-1}} = k - c_{(1-g)^{-1}}. \tag{3.3.7}$$

Note that $(SS^{(-1)})^{(-1)} = SS^{(-1)}$. Hence, for each $h \in \mathbb{F}_q^*$,

$$a_h = a_{h^{-1}}. \tag{3.3.8}$$

Note also that

$$(1-g)(1-g)^{-1} = 1 \implies -g(1-g)^{-1} = 1 - (1-g)^{-1}$$

$$\implies (-g^{-1}(1-g))^{-1} = 1 - (1-g)^{-1} \implies$$

$$(1-g^{-1})^{-1} = 1 - (1-g)^{-1}. \tag{3.3.9}$$

It follows from equations (3.3.8) and (3.3.9) that when we perform the equation arithmetic (3.3.5) + (3.3.6) − (3.3.7), we obtain

$$2a_g = k + c_{(1-g)^{-1}} - c_g - c_{g^{-1}}. \tag{3.3.10}$$

Since for each $h \in \mathbb{F}_q^*$, c_h is either 0 or 1 and since a_g must be an integer, the

result follows from equation (3.3.10). $\square$

Note that for a given $g \in \mathbb{F}_q^* \setminus \{1\}$, the answer to the question of whether or not $g \in R$ depends on equation (3.3.10). Indeed, there is no known simple, explicit description of the set R. However, computations of S and R for specific values of q show that, in general, S is neither a relative difference set nor a partial difference set. Finally, we remark that although we are unable to obtain an entirely satisfactory description of the set R, the *size* of R can be determined by a straightforward counting argument. Indeed, if k is odd, then $|R| = (3q-5)/4$, and if k is even, then $|R| = (q-1)/4$ (see [6]).

We say that t is a *multiplier* of A if there exists $\gamma \in G$ such that $A^{(t)} = \gamma A$, and we say that t is a *strong multiplier* of A if $A^{(t)} = A$. Let A^c denote the complement of A in G. Note that t is a multiplier of A if and only if t is a multiplier of A^c. The elements of $(\mathbb{Z}/v\mathbb{Z})^*$ which are multipliers of A form a group; we refer to this group as the *multiplier group* H of A. Similarly, the elements of $(\mathbb{Z}/v\mathbb{Z})^*$ which are strong multipliers also form a group; we refer to this group as the *strong multiplier group* H_0 of A.

Let E be an almost difference set, and let $\mathbf{e}$ be the sequence corresponding to E. Then $E^{(t)}$ is the group ring element corresponding to the decimation $\mathbf{e}[t']$ of $\mathbf{e}$ (and to the multiple of E by t). Furthermore, t is a multiplier of E if and only if $\mathbf{e}[t']$ is a shift of $\mathbf{e}$; likewise, t is a strong multiplier of E if and only if $\mathbf{e}[t'] = \mathbf{e}$.

Let I be a complete set of distinct coset representatives of H. The set

$\{\mathbf{e}(t') : t \in I\}$ is a maximal set of shift-inequivalent decimations of $\mathbf{e}$. Thus, the problem of determining the shift-inequivalent decimations of $\mathbf{e}$ is equivalent to the problem of determining the multiplier group H.

Because of the connection between Singer difference sets and m-sequences, it is clear from Theorem 2.3.6 that when $p = 2$, the multiplier group of a Singer difference set is $\langle 2 \rangle$. Indeed, it is known that the multiplier group of a Singer difference set defined over $\mathbb{F}_p$ is $\langle p \rangle$ (see [41]).

The use of characters in the study of difference sets dates back to the work of Marshall hall in the 40s (see [43]). As Beth et al mention [12, p. 315], this approach became standard after the paper of Turyn from 1965 [91].

Notation 3.3.2. *Let n be a positive integer. We write ζ_n to denote a primitive, complex nth root of unity.*

Let G be a cyclic group of order v. A *group character* is a homomorphism $\chi : G \to \langle \zeta_v \rangle$. Such a homomorphism can be extended by linearity to a map from $\mathbb{Z}[G]$ to $\mathbb{Z}[\zeta_v]$, the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_v)$ of order v [81, p. 265-268].

The *order* of the character χ is equal to the largest order of the complex roots of unity $\chi(g)$ (as g ranges over G). It is known that for each $n|v$, there exist exactly $\phi(n)$ characters defined on G having order n.

Notation 3.3.3. *The characters of a group G of order v themselves form a group of order v, which we shall denote $\widehat{G}$.*

We will make use of the following result, commonly known as the *in-*

version formula, relating character values to group ring elements (see [12, Lemma VI.3.5]).

Lemma 3.3.4. *Let G be a cyclic group of order v, and let $A \in \mathbb{Z}[G]$. Then the coefficients of A can be recovered from $\chi(A)$ as follows. For $h \in G$,*

$$a_h = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\chi(h^{-1}).$$

Consequently, if for $A, B \in \mathbb{Z}[G]$ $\chi(A) = \chi(B)$ for every $\chi \in \widehat{G}$, then $A = B$.

Using Lemma 3.3.4 in conjunction with (3.3.2), it is easy to see that $D \subseteq G$ is a (v, k, λ) cyclic difference set in G if and only if for each nontrivial $\chi \in \widehat{G}$,

$$|\chi(D)|^2 = k - \lambda.$$

Characters allow us to translate questions about difference sets and almost difference sets to questions about cyclotomic integers. Thus, they allow us to bring tools from algebraic number theory to bear on questions about periodic binary sequences. In the next section, we give an overview of the facts about algebraic number fields that we shall need in the sequel.

3.4 Background from Algebraic Number Theory

An *algebraic number field* K is an extension of $\mathbb{Q}$ in which each element is the root of a polynomial with rational coefficients. The ring of (algebraic) integers of K is the subring $\mathcal{O}_K$ of K consisting of all elements that are roots of monic polynomials with integral coefficients. Let v be a positive integer. Then the cyclotomic field $\mathbb{Q}(\zeta_v)$ is (obviously) an algebraic number field, and it is known that $\mathbb{Z}[\zeta_v]$ (the ring of all integer linear combinations of the vth roots of unity) is its ring of integers (see, for instance, [81, p. 265-268]). Algebraic number fields are primarily used as a tool for studying the integers; indeed, cyclotomic fields were originally defined and studied by mathematicians trying to prove Fermat's Last Theorem (see [31, Chapter 18] for a history).

Many early false proofs of Fermat's last theorem were based on the incorrect assumption that the rings of integers of cyclotomic fields are unique factorization domains (again, see [31, Chapter 18]); this is not so. However, it is known that the rings of integers of cyclotomic fields are Dedekind domains (indeed, all rings of algebraic integers are Dedekind domains; see, for instance, [3, Theorem 8.1.1]). So, every ideal in $\mathbb{Z}[\zeta_v]$ factors uniquely as a product of prime ideals.

For each $j \in (\mathbb{Z}/v\mathbb{Z})^*$, let σ_j denote the automorphism of $\mathbb{Q}(\zeta_v)$ that maps ζ_v to $\zeta_v^{j'}$. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q}) = \{\sigma_j | j \in (\mathbb{Z}/v\mathbb{Z})^*\}$ (see, for example,

[53, Proposition 13.2.1]). This result is important for our investigation of the multiplier groups of the SLCE almost difference sets.

The following technical result, which is stated as Theorem 2.1.9 in [11], also plays a crucial role in our investigation of these multiplier groups.

Lemma 3.4.1. *Let m be a positive integer greater than* 1. *Then the norm of $1-\zeta_m$ in $\mathbb{Q}(\zeta_m)$ is given as follows:*

$$N(1-\zeta_m) = \begin{cases} \ell & \text{if } m \text{ is a power of a prime } \ell, \\ 1 & \text{otherwise.} \end{cases}$$

Let m and v be positive integers greater than 1, and let $m|v$. It follows from the Fundamental Theorem of Galois Theory (specifically, [26, Theorem 14.14, (3)]) that $\mathbb{Q}(\zeta_v)/\mathbb{Q}(\zeta_m)$ is Galois (say, with Galois group H). Furthermore, by [26, Theorem 14.14, (4)], $\mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. So, if N_v denotes the norm in $\mathbb{Q}(\zeta_v)$ and N_m denotes the norm in $\mathbb{Q}(\zeta_m)$, then

$$\begin{aligned} N_v(1-\zeta_m) &= \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})} \sigma(1-\zeta_m) \\ &= \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} \sigma(1-\zeta_m)^{\phi(v)/\phi(m)} \\ &= N_m(1-\zeta_m)^{\phi(v)/\phi(m)}. \end{aligned}$$

Thus, we obtain the following corollary of Lemma 3.4.1.

Corollary 3.4.2. *Let v and m be positive integers greater than* 1, *and let*

$m|v$. Then the norm of $1-\zeta_m$ in $\mathbb{Q}(\zeta_v)$ is given as follows:

$$N(1-\zeta_m) = \begin{cases} \ell^{\phi(v)/\phi(m)} & \text{if } m \text{ is a power of a prime } \ell, \\ 1 & \text{otherwise.} \end{cases}$$

The next theorem gives the prime ideal factorization of the principal ideal generated by a prime number in the ring of integers of a cyclotomic field. Furthermore, it shows how cyclotomic fields can be used to construct finite fields (see, for instance, [53, Theorem 13.2.2]). This connection between cyclotomic fields and finite fields is important for both of our lines of inquiry in this thesis.

Theorem 3.4.3. *Let p be a prime, let $q = p^d$, for some positive integer d, and let k be a positive integer that is not divisible by p. Suppose further that d is the order of $p \pmod{k}$. Also, let P be a prime ideal lying over $\langle p \rangle$ in $\mathbb{Z}[\zeta_k]$, and let T be a set of distinct coset representatives of $\langle p \rangle$ in $(\mathbb{Z}/k\mathbb{Z})^*$. Then*

$$\langle p \rangle = \prod_{j \in T} \sigma_j(P).$$

Additionally, $\mathbb{Z}[\zeta_k]/P \cong \mathbb{F}_q$, and the set $\{\zeta_k^i + P | 0 \leq i < k\}$ contains all k of the kth roots of unity in $\mathbb{Z}[\zeta_k]/P$.

We are also interested in another class of algebraic number fields: quadratic fields (i.e. degree two extensions of $\mathbb{Q}$). These fields play an important role in number theory, particularly in the search for integral solutions to certain

Diophantine equations (see, for instance, [3, Section 14.2]).

The following result relates quadratic and cyclotomic fields. It is because of this result that we able to employ facts about quadratic fields in our study of SLCE almost difference sets, even though the character values of these difference sets are elements of cyclotomic fields. See [53, p. 199] for a proof.

Theorem 3.4.4. *Let ℓ be a prime. Then $\mathbb{Q}\big(\sqrt{(-1)^{(\ell-1)/2}\ell}\ \big)$ is the unique quadratic field contained in the cyclotomic field $\mathbb{Q}(\zeta_\ell)$.*

It is well known that for any quadratic field K, there exists a unique square-free integer n such that $K = \mathbb{Q}(\sqrt{n})$, see [3, p. 95] or [53, p. 188].

An integral basis of a ring of algebraic integers $\mathcal{O}_K$ is a subset $\mathcal{B} = \{b_1, ..., b_t\}$ of $\mathcal{O}_K$ such that each element of $\mathcal{O}_K$ can be written as an integer linear combination of elements of $\mathcal{B}$ in a unique way. Knowing an integral basis for a ring of algebraic integers greatly facilitates computations in that ring of integers. The following result specifies the rings of integers of a certain class of quadratic fields and it gives integral bases for these rings (see [3, p. 96] or [53, p. 189]).

Theorem 3.4.5. *Let $n \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{n})$ be a quadratic field. Then the ring O_K of algebraic integers in K is given by*

$$O_K = \mathbb{Z} + \mathbb{Z}\big(\frac{-1+\sqrt{n}}{2}\big).$$

The next result tells us how the principal ideal generated by 2 factors in

certain quadratic fields; it is a special case of Theorem 10.2.1 from [3, pp. 242-245].

Theorem 3.4.6. *Let $K = \mathbb{Q}(\sqrt{n})$ be a quadratic field. If $n \equiv 1 \pmod 8$, then the ideal $\langle 2 \rangle$ factors into a product of two prime ideals as*

$$\langle 2 \rangle = P_1 P_2 = \langle 2, \frac{1}{2}(1 + \sqrt{n}) \rangle \langle 2, \frac{1}{2}(1 - \sqrt{n}) \rangle.$$

Further, O_K/P_i is a finite field of order 2 for $i = 1, 2$.

Let $K = \mathbb{Q}(\sqrt{n})$ be a quadratic field. It is known that the set $I(K)$ of all nonzero fractional and integral ideals of K forms an Abelian group under multiplication [3, Theorem 8.3.4]. Let $P(K)$ be the subgroup consisting of principal ideals. The quotient group $H(K) = I(K)/P(K)$ is finite [3, Theorem 12.5.4]. We call the order of this group the *class number* of the field K and refer to it as $h(K)$.

There are algorithms for computing the class number of a given quadratic field (see, for example, [3, p. 315]). Furthermore, Dirichlet has shown that class numbers of quadratic fields can be expressed as the evaluations of certain sums of Legendre symbols [3, Theorem 12.6.1].

Class numbers play an important role in many number theoretic investigations, and they also make an appearance in some of our results in this thesis.

3.5 Some applications of the character method

The character method (i.e. the character theoretic approach by which algebraic number theory is used to study difference sets and related combinatorial objects) is perhaps best known as a technique for proving non-existence results about difference sets (see, for instance, the papers of Turyn [91] and Schmidt [83]). However, we use this method to prove structural results concerning the SLCE almost difference sets. In this section, we give an outline of the techniques we use to prove our results.

3.5.1 Galois conjugates and multipliers

Multipliers have two distinct uses in the theory of difference sets. On the one hand, determining the multiplier group of a known class of difference sets yields maximal sets of shift-inequivalent decimations of the sequences associated with those difference sets. On the other hand, it turns out that if one can guarantee that difference sets having certain parameters must have a certain multiplier, then one can sometimes prove that difference sets with those parameters do not exist (see, for instance, [12]). Consequently, multipliers have been studied intensively by difference set theorists. Many different methods have been employed to study these objects (again, see [12]) including a character theoretic approach.

For example, Xiang makes use of characters and algebraic number theory to prove multiplier theorems in [98]. An early version of this approach can

also be found in a paper by Yamamoto from 1963 [99].

Let v is a positive integer, and let $t \in (\mathbb{Z}/v\mathbb{Z})^*$, so that $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_v))$. Let $G = \mathbb{Z}/v\mathbb{Z}$. If t is a multiplier of $A \in \mathbb{Z}[G]$, then there exists $\gamma \in G$ such that $A^{(t)} = \gamma A$. Consequently, for each character χ of G,

$$\sigma_t(\chi(A)) = \chi(A^{(t)}) = \chi(\gamma A) = \chi(\gamma)\chi(A) = \zeta\chi(A), \tag{3.5.1}$$

for some (not necessarily primitive) vth root of unity ζ.

The group of all Galois conjugates fixing an ideal I of $\mathbb{Z}[\zeta_v]$ is called the *decomposition group* of I. It follows from Equation 3.5.1 that the multiplier group H of A is a subgroup of the decomposition group of $\langle\chi(A)\rangle$ (where χ is any character of G).

In Chapter 5, we prove some results concerning the multiplier group of an SLCE almost difference set S by determining the decomposition group of $\langle\chi(S)\rangle$ (for certain characters χ).

3.5.2 Prime ideals and linear complexity *

Let $\mathbf{a} = a_0a_1a_2...$ be a binary sequence of period v, and let $A(x) = \sum_{i=0}^{v-1} a_ix^i \in \mathbb{F}_2[x]$. Recall that by Theorem 2.1.13, the linear complexity of $\mathbf{a}$ is $v - \deg(\gcd(A(x), x^v - 1))$. So, if one can compute $\gcd(A(x), x^v - 1)$, then one can determine the linear complexity of $\mathbf{a}$. Furthermore, even if one cannot completely calculate this gcd, simply proving that some polynomial $p(x)$ divides $\gcd(A(x), x^v - 1)$ yields an upper bound on the linear complexity of

a.

If 2 does not divide v, then $x^v - 1$ splits into distinct linear factors in some extension of $\mathbb{F}_2$; however, if $2|v$, then this is not the case [66, Theorem 2.42]. Thus, it is easier to determine $\gcd(A(x), x^v - 1)$ when 2 does not divide v than when $2|v$. For, if 2 does not divide v, then one simply needs to determine the linear factors of $\gcd(A(x), x^v - 1)$, while if $2|v$, one needs to determine both which linear polynomials divide $\gcd(A(x), x^v - 1)$ and the multiplicity with which they divide it. This may partially explain why the problem of determining the linear complexity of the SLCE sequences is still open (since these sequences have even periods).

Several authors have used a character-theoretic approach to determine the linear complexity of certain classes of sequences of odd period. For example, this approach was applied successfully by MacWilliams and Mann [68] as well as by Evans, Hollmann, Krattenthaler, and Xiang [29]. These authors make use of the following theorem to obtain their results [12, Lemma VI.17.16].

Theorem 3.5.1. *Let v be an odd, positive integer, let* **a** *be a binary sequence of period v, let $G = \mathbb{Z}/v\mathbb{Z}$, and let $A \in \mathbb{Z}[G]$ be the group ring element corresponding to* **a**. *Let $\mathcal{P}$ be a prime ideal lying above 2 in $\mathbb{Z}[\zeta_v]$. Then the linear complexity of* **a** *is equal to the number of characters χ of G for which $\chi(A) \not\equiv 0 \pmod{\mathcal{P}}$.*

In order to study the linear complexity of the SLCE sequences, we make use of a rather obvious refinement of Theorem 3.5.1, which, to the best of our knowledge, originally appeared in our paper [2]. In what follows, we

assume that q is an odd prime power, $\mathbf{s} = s_0 s_1 s_2 ...$ is an SLCE sequence over $\mathbb{F}_q^*$, and $S_2(x) := \sum_{i=0}^{q-2} s_i x^i \in \mathbb{F}_2[x]$. We wish to (at least partially) calculate $\gcd(S_2(x), x^{q-1} - 1)$

Notation 3.5.2. *Let $k|q-1$ ($k \geq 3$) and let f be the order of k mod 2. Since $\mathbb{F}_{2^f}^*$ is a cyclic group of order $2^f - 1$, it has a subgroup of order k. Hence, the polynomial $x^k + 1 = (1+x)(1+x+\cdots+x^{k-1})$ splits completely over $\mathbb{F}_{2^f}$. Let $\beta \in \mathbb{F}_{2^f}$ be an element of order k, so that β is a root of $1+x+\cdots+x^{k-1}$. Let $I_\beta(x)$ be the minimal polynomial of β over $\mathbb{F}_2$.*

Note that $I_\beta(x)|1+x+\cdots+x^{k-1}$; indeed, $1+x+\cdots+x^{k-1}$ is a product of distinct minimal polynomials of elements of $\mathbb{F}_{2^f}$ of order dividing k. Since $k|q-1$, β is a root of $x^{q-1}+1$, and so $I_\beta(x)$ is a factor of $x^{q-1}+1$ (and, indeed, $1+x+\cdots+x^{k-1}|x^{q-1}+1$). We want to determine whether or not $I_\beta(x)$ and/or $1+x+\cdots+x^{k-1}$ divide $S_2(x)$. Note that $I_\beta(x)|S_2(x)$ if and only if $S_2(\beta) = 0$, where $S_2(\beta)$ is an element of $\mathbb{F}_{2^f}$.

Let $\mathcal{P}$ be a prime ideal lying over 2 in $\mathbb{Z}[\zeta_k]$. By Theorem 3.4.3, we have $\mathbb{F}_{2^f} \simeq \mathbb{Z}[\zeta_k]/\mathcal{P}$. Let $\phi : \mathbb{F}_{2^f} \to \mathbb{Z}[\zeta_k]/\mathcal{P}$ be an isomorphism. Of course, $\phi(0) = 0 + \mathcal{P}$ and $\phi(1) = 1 + \mathcal{P}$. Since β has order k, there exists $\eta \in \mathbb{F}_{2^f}$ such that $\beta = \eta^{(2^f-1)/k}$, and, consequently, $\phi(\beta) = \phi(\eta)^{(2^f-1)/k}$. Hence, there exists a unique (in this case, primitive) kth root of unity congruent to $\phi(\beta)$ (mod $\mathcal{P}$).

Let ζ denote the unique primitive kth root of unity congruent to $\phi(\beta)$ (mod $\mathcal{P}$). Let χ denote the unique group character mapping α to ζ. Let

$S_z(x)$ be the polynomial in $\mathbb{Z}[x]$ obtained by replacing each coefficient of $S_2(x)$ with its counterpart (0 or 1) from $\mathbb{Z}$.

We note that $\phi(S_2(\beta))$ is the equivalence class modulo $\mathcal{P}$ containing $S_z(\zeta)$, and

$$\chi(S) + \mathcal{P} = S_z(\zeta) + \mathcal{P} = \phi(S_2(\beta)).$$

Hence,

$$I_\beta(x)|S_2(x) \iff \chi(S) \equiv 0 \pmod{\mathcal{P}}. \tag{3.5.2}$$

Thus, even though the periods of the SLCE sequences are even, we can still use characters to determine the divisors of $\gcd(S_2(x), x^{q-1} - 1)$. However, as it stands, our method tells us nothing about the multiplicity with which these divisors factor into this gcd.

We conclude this section by deducing a slightly modified version of (3.5.2), which is more convenient for our purposes. Since χ is nontrivial, we have $\chi(S) = \chi(G - S^c) = -\chi(S^c)$, so that

$$\chi(S) \equiv 0 \pmod{\mathcal{P}} \iff \chi(S^c) \equiv 0 \pmod{\mathcal{P}}.$$

Hence, we have deduced the following result.

$$I_\beta(x)|S_2(x) \iff \chi(S^c) \equiv 0 \pmod{\mathcal{P}}. \tag{3.5.3}$$

Chapter 4

Gauss and Jacobi sums

Let p be a prime, d a positive integer, and $q = p^d$. Let α be a primitive element of $\mathbb{F}_q$. Let χ be a character on $\mathbb{F}_q^*$. It is common to extend χ to a map on $\mathbb{F}_q$ by setting $\chi(0) = 0$. The *Gauss sum* $G(\chi)$ is the character sum

$$G(\chi) := \sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) e^{2\pi i (\mathrm{tr}(\alpha))'/p},$$

where tr is the field trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. If $|\chi| = k$, then we say that $G(\chi)$ is a *Gauss sum of order* k.

Gauss sums have many applications, both in number theory and information theory (see [76, Introduction] for a summary of some of the many uses of these character sums). Of course, Gauss sums were originally considered by C. F. Gauss, who made use of them in two of his proofs of the law of quadratic reciprocity (see [53, Section 6.3] for a slight variant of one of Gauss' proofs).

The ideas behind Gauss's proofs can be applied more generally: Gauss sums can be used to prove several higher reciprocity laws. See [53, Chapters 9 and 14] for an account of the use of Gauss sums in proving reciprocity laws.

Let χ and ϕ be characters of $\mathbb{F}_q$. The Jacobi sum $J(\chi, \phi)$ is the character sum

$$J(\chi, \phi) := \sum_{i=0}^{q-2} \chi(\alpha^i)\phi(1 - \alpha^i).$$

If $\text{lcm}(|\chi|, |\phi|) = m$, then we say that $J(\chi, \phi)$ is a *Jacobi sum of order* m.

Jacobi sums also have many applications in number theory and information theory (again, see [76, Introduction]). Of course, Jacobi sums were originally considered by C. G. J. Jacobi. A. Weil [93] showed that these sums have a natural application to the problem of counting the number of solutions to certain equations over finite fields (see [53, Sections 8.3-8.7] for an account of Weil's technique).

For many applications, it would be useful to be able to evaluate Gauss and Jacobi sums explicitly. However, while it is easy to show that if the characters involved in either type of sum are nontrivial, then the sum in question has absolute value $\sqrt{q}$ (see, for instance, [53, Proposition 8.2.2 and Theorem 8.3.1(d)]) in general, the exact values of these sums are not known. But Gauss and Jacobi sums have been evaluated in certain special cases; these evaluations play an important role in our study of the linear complexity of the SLCE sequences. We give a brief account of the known evaluations of Gauss and Jacobi sums later in this chapter.

Let χ be a character of order k on $\mathbb{F}_q$, and let ρ be the quadratic character on $\mathbb{F}_q$. We are particularly interested in the Jacobi sum

$$K(\chi) := J(\chi, \rho).$$

This Jacobi sum plays a fundamental role in the derivation of explicit formulae for Jacobi sums of order k. The usual strategy for evaluating Jacobi sums is to first evaluate $K(\chi)$ directly, and then use the resulting formulae in concert with certain identities relating different Jacobi sums to one another to obtain formulae for other Jacobi sums (see [11, Chapter 3]).

It is known (see, for instance, [11, Theorem 2.1.4]) that

$$K(\chi) := \chi(4)J(\chi, \chi).$$

This alternative formulation of $K(\chi)$ is actually more useful for our purposes. We also make note of the following useful fact about these sums (see [11, Theorem 2.1.8]).

Lemma 4.0.1. *Let q be an odd prime power, and let χ be a character on $\mathbb{F}_q$ of order $k > 1$. Then*

$$K(\chi) \equiv -q \pmod{2(1 - \zeta_k)}.$$

Finally, we state a formula that gives a relation between certain Gauss and Jacobi sums (see [53, Theorem 8.3.1(d)]). If χ, ϕ, and $\chi\phi$ are non-trivial

characters on $\mathbb{F}_q$, then

$$J(\chi, \phi) = \frac{G(\chi)G(\phi)}{G(\chi\phi)}. \tag{4.0.1}$$

In particular, if χ is a character of order greater than 2, we have

$$K(\chi) = J(\chi, \rho) = \frac{G(\rho)G(\chi)}{G(\chi\rho)}. \tag{4.0.2}$$

4.1 Stickelberger's Theorem

Stickelberger's congruence gives a congruence for Gauss sums in certain extensions of $\mathbb{Q}$ (see [11, Theorem 11.2.1]). Stickelberger's theorem, which is a direct consequence of Stickelberger's congruence, describes the prime ideal factorizations of Jacobi sums and certain powers of Gauss sums in cyclotomic fields (see [11, Theorem 11.2.2 and Theorem 11.2.3]). Stickelberger's theorem is the basis of most known evaluations of Gauss and Jacobi sums (see, for example, the evaluations Gauss and Jacobi sums of small order given in [11, Chapters 3 and 4] or the evaluations of small index Gauss sums given in [61]). Furthermore, it plays a crucial role in our study of the multiplier groups of the SLCE sequences. In this section, we describe a special case of this important result.

For the rest of this section, let p be a prime, let k be a positive integer that is not divisible by p, let d be the order of $p \pmod{k}$, and let $q = p^d$. Furthermore, let P be a prime ideal lying over (p) in $\mathbb{Z}[\zeta_k]$, and let T be a set of distinct coset representatives of $\langle p \rangle$ in $(\mathbb{Z}/k\mathbb{Z})^*$.

Recall that by Theorem 3.4.3, $\mathbb{Z}[\zeta_k]/P \cong \mathbb{F}_q$, and the set $\{\zeta_k^i + P | 0 \leq i < k\}$ contains all k of the kth roots of unity in $\mathbb{Z}[\zeta_k]/P$. Let $\chi_P : \mathbb{Z}[\zeta_k]/P \to \mathbb{C}$ be the function defined by the rule that for $\alpha + P \in \mathbb{Z}[\zeta_k]/P$, $\chi(\alpha + P) = \zeta_k^i$, where ζ_k^i is the unique power of ζ_k congruent to $\alpha^{(q-1)/k} \pmod{P}$. Then χ_P is called a *Techimuller character*. Any character of order k on $\mathbb{F}_q$ can be viewed as a Techimuller character by identifying a generator $\alpha+P$ of $(\mathbb{Z}[\zeta_k]/P)^*$ with a generator γ of $\mathbb{F}_q^*$ such that $\chi_P(\alpha + P) = \chi(\gamma)$.

The next theorem, which gives the prime ideal factorization of $(K(\chi))$ in $\mathbb{Z}[\zeta_k]$, is a consequence of Stickelberger's Theorem (see [11, Corollary 11.2.4 and Theorem 11.2.9]).

Theorem 4.1.1.

$$(K(\chi_P)) = \prod_{j \in T} \sigma_{j^{-1}}(P)^{d - \sum_{i=0}^{d-1} \{\lfloor \frac{2j'p^i}{k} \rfloor - 2\lfloor \frac{j'p^i}{k} \rfloor\}}.$$

As the authors of [11] note, the term $\{\lfloor \frac{2j'p^i}{k} \rfloor - 2\lfloor \frac{j'p^i}{k} \rfloor\}$ appearing in Theorem 4.1.1 equals 1 or 0 according to whether the remainder upon dividing $j'p^i$ by k is greater than $k/2$ or not.

4.2 Explicit evaluations of Gauss and Jacobi sums

There are three cases in which there are known evaluations of Gauss and Jacobi sums: the small order case, the pure case, and the small index case.

4.2.1 Gauss and Jacobi sums of small order

Explicit evaluations of Gauss and Jacobi sums over certain characters of small order have been computed. See [11, Chapters 3 and 4] for an overview of many such computations.

The first such evaluation was given by Gauss himself, who gave formulae for the so-called quadratic Gauss sums over prime fields (see [11, Theorem 1.2.4] for a proof).

Theorem 4.2.1. *Let p be an odd prime, and let ρ be the quadratic character of $\mathbb{F}_p$. Then*

$$G(\rho) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Gauss's formulae for the quadratic Gauss sums can be extended to finite fields $\mathbb{F}_q$ of odd order using a result called the Hasse-Davenport lifting theorem. Let p be an odd prime, d a positive integer, and $q = p^d$. Let $k|q-1$, and let χ be a character on $\mathbb{F}_q$ of order k. Let $m \geq 1$ be an integer, and let $\chi' := \chi \circ N$, where N is the field norm from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Then χ' is a character on $\mathbb{F}_{q^m}$ of order k, which is called a *lifted character*. Note that every character on $\mathbb{F}_{q^m}$ of order k can be obtained as a lifted character from a character of $\mathbb{F}_q$ of order k. We mention the following important identity, which is known as the Hasse-Davenport Lifting Theorem (see [11, Theorem 11.5.2]).

$$G(\chi') = (-1)^{m-1}(G(\chi))^m. \tag{4.2.1}$$

The following is the general formulae for quadratic Gauss sums over finite fields (see [11, Theorem 11.5.4] for a proof).

Theorem 4.2.2. *Let m be a positive integer, and let ρ be the quadratic character on $\mathbb{F}_{p^m}$. Then*

$$G(\rho) = \begin{cases} (-1)^{m-1} p^{m/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{m-1} i^m p^{m/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Most formulae for small order Gauss and Jacobi sums are obtained by the following procedure. First, formulae for sums of the form $K(\chi)$ are computed by representing the sums as integer linear combinations of elements of an integral basis of a cyclotomic field of small order, and then Stickelberger's theorem is used to make inferences about the coefficients in the linear combination. Next, formulae for other Jacobi sums are computed from the formulae for $K(\chi)$ using relations between Jacobi sums of different types. Finally, formulae for Gauss sums are deduced using facts relating Gauss and Jacobi sums to one another, such as (4.0.1). A number of evaluations of Gauss and Jacobi sums are derived in [11, Chapters 3 and 4] using this method. Unfortunately, this procedure becomes increasingly more difficult to execute, and the resulting formulae become increasingly complicated and more difficult to apply, as one considers Gauss and Jacobi sums over characters of increasingly large order.

As an example of the types of evaluations one can obtain for Gauss and

Jacobi sums of small order, we state the following result (see [11, Theorem 3.1.3] for a proof).

Theorem 4.2.3. *Let p be an odd prime congruent to 1 mod 3, and let g be a primitive root of $\mathbb{F}_p^*$. Let χ be a character of order 3 on $\mathbb{F}_p$. Then*

$$K(\chi) = \frac{1}{2}(r + si\sqrt{3}),$$

where r and s are integers such that $r^2 + 3s^2 = 4p$, $r \equiv 1 \pmod 3$, $s \equiv 0 \pmod 3$, and $3s \equiv (2g^{(p-1)/3} + 1)r \pmod p$.

4.2.2 Pure Gauss and Jacobi sums *

A Gauss sum is called *pure* if some positive integral power of it is real. Pure Gauss sums were first considered by Stickelberger in the 1890s. The following theorem, which is partially due to his work, completely classifies pure Gauss sums (see [11, Section 11.6]).

Theorem 4.2.4. *Let p be a prime, let m be a positive integer, and let $q = p^m$. Let $n|q-1$, and let ϵ be a character of order n on $\mathbb{F}_q$. Then $G(\epsilon)$ is pure if and only if there exists a positive integer x such that*

$$p^x \equiv -1 \pmod n. \tag{4.2.2}$$

Furthermore, if there exist integers satisfying (4.2.2) and t is the least

such integer, then there exists a positive integer s such that $m = 2ts$, and

$$G(\epsilon) = (-1)^{s-1+(p^t+1)s/n} p^{m/2}.$$

A Jacobi sum is also called *pure* if some positive integral power of it is real. Pure Jacobi sums of the form $K(\chi)$ were studied in [1] and [85]. The authors of [1] and [85] showed that if m is odd, then no Jacobi sum defined on $\mathbb{F}_{p^m}$ can be pure. They also completely determined conditions under which Jacobi sums are pure when $m = 2$.

Theorem 4.2.5. *Let p be a prime, $m = 2$, and $q = p^m$. Let χ be a character on $\mathbb{F}_q$ of order k. Then $K(\chi)$ is pure if and only if k is a divisor of $p + 1$, k is an even divisor of $2(p - 1)$, $k = 24$ and $p \equiv 17, 19 \pmod{24}$, or $k = 60$ and $p \equiv 41, 49 \pmod{60}$.*

In the case that k is odd, an explicit evaluation of $K(\chi)$ is given in [10, Theorem 2.14].

Theorem 4.2.6. *Let $m = 2$, and let k be an odd divisor of $p + 1$. Then $K(\chi) = p$.*

However, rather than make direct use of the results from [1], [85], and [10], which apply only to finite fields of the form $\mathbb{F}_{p^2}$, we use Theorem 4.2.4 in conjunction with the extension of Gauss's evaluation of the quadratic Gauss sums given in Theorem 4.2.2 and (4.0.2) to obtain formulae for pure Jacobi sums of the form $K(\chi)$ that apply much more generally.

Let p be an odd prime, m a positive integer, and $q = p^m$. Let k be an odd divisor of $q-1$, χ a character on $\mathbb{F}_q$ of order k, and ρ the quadratic character on $\mathbb{F}_q$. We now assume that there exists a positive integer x such that $p^x \equiv -1 \pmod{k}$; indeed, we refer to the least such integer as t. Then, by Theorem 4.2.4, $G(\chi)$ is a pure Gauss sum. Since k is odd and p^t+1 is even, then $k|p^t+1 \iff 2k|p^t+1$. Hence, since t is the smallest positive integer satisfying $p^t \equiv -1 \pmod{k}$, then t is also the smallest positive integer satisfying $p^t \equiv -1 \pmod{2k}$. We note that $\chi\rho$ is a character of order $\operatorname{lcm}(2,k) = 2k$. Thus, $G(\chi\rho)$ is a pure Gauss sum. So, in this case, we can use Theorem 4.2.4, (4.2.2), and (4.0.1) to evaluate the Jacobi sum $K(\chi)$. We note that by Theorem 4.2.4, $m = 2ts$ for some positive integer s. Since the evaluation in (4.2.2) breaks into two cases, our evaluation also breaks into two cases.

First, we assume that $p \equiv 1 \pmod{4}$. Then

$$K(\chi) = \frac{(-1)^{m-1}p^{m/2}(-1)^{s-1+(p^t+1)s/k}p^{m/2}}{(-1)^{s-1+(p^t+1)s/(2k)}p^{m/2}} = (-1)^{1+(p^t+1)s/(2k)}p^{m/2}.$$

Let us consider the special case in which $m = 2$ and $k|p+1$ (so that $t = s = 1$). Since $p \equiv 1 \pmod{4}$, it follows that $(p^t+1)/2k$ is odd. Then by Theorem 4.2.6, the evaluation of $K(\chi)$ given above reduces to the evaluation $K(\chi) = p$.

Next, we assume that $p \equiv 3 \pmod{4}$. Then

$$K(\chi) = \frac{(-1)^{m-1}i^m p^{m/2}(-1)^{s-1+(p^t+1)s/k}p^{m/2}}{(-1)^{s-1+(p^t+1)s/(2k)}p^{m/2}} = (-1)^{1+m/2+(p^t+1)s/(2k)}p^{m/2}.$$

Again, let us consider the special case in which $m = 2$ and $k|p+1$ (so that $s = t = 1$). Since $p \equiv 3 \pmod 4$, it follows that $(p^t+1)/2k$ is even. Then by Theorem 4.2.6, the evaluation of $K(\chi)$ given above reduces to the evaluation $K(\chi) = p$.

Corollary 4.2.7. *Let p be a an odd prime, let m be a positive integer, and let k be an odd divisor of $p^m - 1$. Let χ be a character of order k on $\mathbb{F}_{p^m}$. Assume that there exist positive integers x such that $p^x \equiv -1 \pmod k$, and let t be the least such integer. Then there exists $s \in \mathbb{N}$ such that $m = 2ts$, and*

$$K(\chi) = \begin{cases} (-1)^{1+(p^t+1)s/(2k)} p^{m/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{1+m/2+(p^t+1)s/(2k)} p^{m/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

4.2.3 Small index Gauss and Jacobi sums *

Finally, a third case in which there are known evaluations for Gauss and Jacobi sums is that of the small index Gauss and Jacobi sums. We will discuss the sums $K(\chi)$ in this context. As usual, let p be an odd prime, m a positive integer, $q = p^m$, and α a primitive element of $\mathbb{F}_q$. Let k be an odd divisor of $q-1$, and let χ be a character on $\mathbb{F}_q$ of order k. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_k)) \cong (\mathbb{Z}/k\mathbb{Z})^*$. Let $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_k))$ be the automorphism mapping ζ_k to ζ_k^p. Then, since the Froebenius map is an automorphism of $\mathbb{F}_q$ fixing

the elements of $\mathbb{F}_p$, we have that

$$\begin{aligned}\sigma_p(K(\chi)) &= \sigma_p(\chi(4))\sum_{i=1}^{q-2}\sigma_p(\chi(\alpha^i))\sigma_p(\chi(1-\alpha^i)) \\ &= \chi(4^p)\sum_{i=1}^{q-2}\chi((\alpha^i)^p)\chi(1^p-(\alpha^i)^p) \\ &= \chi(4)\sum_{i=1}^{q-2}\chi(\alpha^i)\chi(1-\alpha^i) = K(\chi).\end{aligned}$$

Thus, $K(\chi)$ is in the fixed field of σ_p, and by the Fundamental Theorem of Galois Theory, this field has degree $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p\rangle]$ as an extension of $\mathbb{Q}$. Since we know how to evaluate $K(\chi)$ when there exist positive integers x such that $p^x \equiv -1 \pmod{k}$, we can confine ourselves to the case in which there exist no such integers. Having made this assumption, we see that the quotient group $(\mathbb{Z}/k\mathbb{Z})^*/\langle p\rangle$ must contain the (non-identity) element $-1+\langle p\rangle$ and so (by Lagrange's Theorem) must have even order.

The small index assumption is the assumption that $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p\rangle]$ is a small positive integer. By making this assumption, we can infer that $K(\chi)$ lies in an algebraic number field of small degree and can therefore use facts about such number fields to evaluate $K(\chi)$. Explicit evaluations have been obtained for Gauss sums in the index 2 and index 4 cases. It is sometimes possible to translate these Gauss sum evaluations into evaluations of $K(\chi)$.

Let us assume that $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p\rangle] = 2$. It is easy to see that

$$(\mathbb{Z}/k\mathbb{Z})^* \cong \langle p\rangle \times \langle -1\rangle.$$

Thus, $(\mathbb{Z}/k\mathbb{Z})^*$ contains at most 3 elements of order 2, and it follows easily from the Chinese Remainder Theorem that (since k is odd) either $k = \ell_1^{r_1}$ or $k = \ell_1^{r_1}\ell_2^{r_2}$ for some odd primes ℓ_1 and ℓ_2, and some positive integers r_1 and r_2.

The following evaluation is due to Langevin [61]. We note that the congruence condition $\ell \equiv 3 \pmod 4$ is actually forced by the index 2 assumption, as Langevin demonstrates in his paper. Furthermore, the hypothesis in the evaluation below that $\ell > 3$ is only necessary to obtain a nice expression for the Gauss sum in terms of the class number of a certain quadratic field. We have rephrased Langevin's result in the manner in which it was stated in [97].

Theorem 4.2.8. *Let p be an odd prime, let m be a positive integer, and let $k|p^m-1$. Let χ be a character of order k on $\mathbb{F}_{p^m}$. Assume $k = \ell^r$, where $\ell > 3$ is a prime congruent to 3 (mod 4) and r is a positive integer. We suppose that $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle] = 2$ and $m = \phi(k)/2$. Then*

$$G(\chi) = p^{\frac{1}{2}(m-h)} \left(\frac{a + b\sqrt{-\ell}}{2} \right),$$

where $h = h(\mathbb{Q}(\sqrt{-\ell}))$ is the class number of $\mathbb{Q}(\sqrt{-\ell})$, and the integers a and b satisfy the three conditions

$$a, b \not\equiv 0 \pmod p,\ 4p^h = a^2 + \ell b^2,\ \text{and } a \equiv -2p^{\frac{1}{2}(m+h)} \pmod \ell.$$

Furthermore, these conditions are sufficient to determine a completely and to determine b up to sign.

In the above formula, in place of the expression $\left(\frac{a+b\sqrt{-\ell}}{2}\right)$, Langevin had originally used the expression $a' + b'\left(\frac{-1+\sqrt{-\ell}}{2}\right)$, where $a', b' \in \mathbb{Z}$. Note that

$$a' + b'\left(\frac{-1+\sqrt{-\ell}}{2}\right) = \frac{(2a'-b') + b'\sqrt{-\ell}}{2}.$$

The integers a and b in the version from [97] (and from Theorem 4.2.8 above) are obtained by setting $a = 2a' - b'$ and $b = b'$. As a result, we also have the condition (not stated explicitly in our version of Theorem 4.2.8) that $a \equiv b \pmod 2$.

Note also that $[(\mathbb{Z}/2k\mathbb{Z})^* : \langle p \rangle] = 2$. Xia and Yang have evaluated index 2 Gauss sums over characters of order $2\ell^r$ [97]. Their result breaks into two separate cases: one in which $\ell \equiv 3 \pmod 8$ and one in which $\ell \equiv 7 \pmod 8$. We only make use of the result for the case in which $\ell \equiv 7 \pmod 8$.

Theorem 4.2.9. *Let p be an odd prime, let m be a positive integer, and let $k|p^m - 1$. Assume that $k = \ell^r$, where $\ell > 3$ is a prime congruent to 7 (mod 8) and r is a positive integer. We supppose that $[(\mathbb{Z}/2k\mathbb{Z})^* : \langle p \rangle] = 2$ and $m = \phi(k)/2$. Let ϵ be a character on $\mathbb{F}_{p^m}$ of order $2k$. Then*

$$G(\epsilon) = (-1)^{r\frac{p-1}{2}}\sqrt{(-1)^{(p-1)/2}}p^{\frac{m}{2}}.$$

Let us make a slight modification to our earlier hypotheses. Assume s is

a positive integer, and let $m = \phi(k)s/2$. So, we are now considering a larger class of prime powers p^m. Let us set $e = \phi(k)/2$, so that $m = es$. Let $\ell \equiv 7 \pmod 8$. We consider two cases.

Case 1: $p \equiv 1 \pmod 4$. By Theorems 4.2.1, 4.2.2, and 4.2.9, we have that

$$K(\chi) = \frac{(-1)^{es-1}p^{es/2}(-1)^{s-1}p^{(e-h)s/2}\left(\frac{a+b\sqrt{-\ell}}{2}\right)^s}{(-1)^{s-1+r(p-1)s/2+(p-1)s/4}p^{es/2}}.$$

Since e is odd and $(p-1)/2$ is even, we deduce that

$$K(\chi) = (-1)^{s-1-(p-1)s/4}p^{(e-h)s/2}\left(\frac{a+b\sqrt{-\ell}}{2}\right)^s.$$

Case 2: $p \equiv 3 \pmod 4$. By Theorems 4.2.1, 4.2.2, and 4.2.9, we have that

$$K(\chi) = \frac{(-1)^{es-1+es/2}p^{es/2}(-1)^{s-1}p^{(e-h)s/2}\left(\frac{a+b\sqrt{-\ell}}{2}\right)^s}{(-1)^{s-1+r(p-1)s/2+(p-1)s/4}p^{es/2}}.$$

Since e and $(p-1)/2$ are odd, we deduce that

$$K(\chi) = (-1)^{s-1-rs+(e+1)s/2}p^{(e-h)s/2}\left(\frac{a+b\sqrt{-\ell}}{2}\right)^s.$$

We collect these observations for later reference.

Corollary 4.2.10. *Let p be an odd prime, let m be a positive integer, and let $k|p^m-1$. Let χ be a character of order k on $\mathbb{F}_{p^m}$. Assume that $k = \ell^r$, where ℓ is a prime congruent to* 7 (mod 8) *and r is a positive integer. We suppose that $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle] = 2$ and $m = \phi(k)s/2$, where s is a positive integer.*

If $p \equiv 1 \pmod 4$, *then*

$$K(\chi) = (-1)^{s-1-(p-1)s/4} p^{(e-h)s/2} \left(\frac{a + b\sqrt{-\ell}}{2} \right)^s .$$

If $p \equiv 3 \pmod 4$, *then*

$$K(\chi) = (-1)^{s-1-rs+(e+1)s/2} p^{(e-h)s/2} \left(\frac{a + b\sqrt{-\ell}}{2} \right)^s .$$

4.3 Jacobi sums, Jacobsthal sums, and cyclotomic numbers

In this section, we briefly explore the connections between Jacobi sums, Jacobsthal sums, and cyclotomic numbers. These connections are relevant to our work in this thesis since we have elected to study the SLCE sequences using Jacobi sums, whereas other authors have made use of cyclotomic numbers and Jacobsthal sums (see, for example, [59] and [73]).

In order to state a formula relating cyclotomic numbers and Jacobi sums, we introduce a slightly altered type of Jacobi sum. In lieu of the definition for $J(\chi, \phi)$ given in 4, we define the Jacobi sum $J^*(\chi, \phi)$ by the rule

$$J^*(\chi, \phi) := \sum_{i=2}^{q-2} \chi(\alpha^i)\phi(1 - \alpha^i).$$

The following theorem relates Jacobi sums and cyclotomic numbers over

prime fields (see [11, Theorem 2.5.1] for a proof).

Theorem 4.3.1. *Let p be a prime, and let k be an integer with $k \geq 2$ such that $k|p-1$. Indeed, let $p = kf + 1$, for some positive integer f. Let g be a fixed primitive root (mod p), let $\beta := e^{(2\pi i)/k}$, and let χ be a character of order k on $\mathbb{F}_p$ such that $\chi(g) = \beta$. For $s, t = 0, 1, ..., k-1$,*

$$k^2(s,t) = \sum_{u=0}^{k-1} \sum_{v=0}^{k-1} (-1)^{uf} \beta^{-su-tv} J^*(\chi^u, \chi^v).$$

Theorem 4.3.1 is the primary tool for evaluating cyclotomic numbers. Hence, the increasing complexity of the formulae for cyclotomic numbers for increasing k is a direct consequence of the increasing complexity of the evaluations of Jacobi sums for increasing k. Note that one must be able to evaluate a number of different Jacobi sums in order to apply this result to find formulae for cyclotomic numbers.

Let q be an odd prime power, and let ρ be the quadratic character on $\mathbb{F}_q$. Following the notation from [59], we stipulate that for $a \in \mathbb{F}_q^*$ and $n \in \mathbb{N}$, the sums

$$I_n(a) := \sum_{c \in \mathbb{F}_q^*} \rho(c^n + a) \text{ and}$$

$$H_n(a) := \sum_{c \in \mathbb{F}_q^*} \rho(c)\rho(c^n + a)$$

are called *Jacobsthal sums*. For some applications of Jacobsthal sums to number theory, see [11, Section 6.3].

The following theorem specifies a connection between Jacobi sums and

Jacobsthal sums over prime fields (see [11, Theorems 6.1.14 and 6.1.15] for a proof).

Theorem 4.3.2. *Let k be a positive integer, and let p be a prime with $p \equiv 1 \pmod{2k}$. Let χ be a character on $\mathbb{F}_p$ of order $2k$, and let ρ be the quadratic (Legendre) character on $\mathbb{F}_p^*$. Then for $a \in \mathbb{F}_p^*$ and $n \in \mathbb{N}$*

$$H_n(a) = \chi(-1) \sum_{j=0}^{k-1} \chi^{k+2j+1}(a) K(\chi^{2j+1}) \text{ and}$$

$$I_n(a) = \rho(a) \sum_{j=1}^{k-1} \chi^{2j}(a) K(\chi^{2j}) - \rho(a).$$

Note that one would have to be able to evaluate many Jacobi sums in order to use Theorem 4.3.2 to evaluate Jacobsthal sums.

4.4 The character formula *

In this section, we explore two uses of Gauss and Jacobi sums in the theory of difference sets, and we prove the formula expressing the character values of the SLCE almost difference sets in terms of Jacobi sums of the form $K(\chi)$ that serves as the cornerstone for our work in this thesis.

Let q be a prime power, d a positive integer, and H_β the Singer difference set defined in (3.1.1). Let χ be a character on $\mathbb{F}_{q^d}$ whose restriction to $\mathbb{F}_q$ is

trivial. Yamamoto [99] proved that

$$\chi(H_\beta) = \frac{1}{q}G(\chi). \tag{4.4.1}$$

He was able to use his formula to obtain an alternative proof that the set H_β *is*, in fact, a difference set. His proof is, in a sense, simpler than the proof given by Singer in [87].

Let k and d be positive integers. Let $H(x^k)$ be the subset of $\mathrm{PG}(2, \mathbb{F}_{2^{d+1}})$ defined by (3.1.2). Assume that $H(x^k)$ is a hyperoval. Let $D(x^k)$ be the set defined by (3.1.3). Let χ be a nontrivial character on $\mathbb{F}_{2^d}$ Evans, Hollmann, Krattenthaller, and Xiang [29] proved that there exists a nontrivial character ϕ on $\mathbb{F}_{2^d}$ such that $\chi = \phi^{k-1}$ and

$$\chi(D(x^k)) = \frac{1}{2}J(\phi, \chi). \tag{4.4.2}$$

Evans et al were able to use their formula to obtain an alternative proof that the set $D(x^k)$ *is*, in fact, a difference set [29]. Their proof is, in a sense, simpler than the proof given by Maschietti [70]. They were also able to use their formula to compute the linear complexities of sequences associated with various hyperovals [29].

We now state and prove our character formula. A version of this result appeared in our recent paper [2].

Theorem 4.4.1. *Let q be an odd prime power, and let $k|q-1$. Let χ be a*

character on $\mathbb{F}_q$, and let S be the SLCE almost difference set in $\mathbb{F}_q^*$. Then

$$\chi(S^c) = \frac{1}{2}\chi(-1)(K(\chi)+1).$$

Proof. The reasoning in the next two sentences is taken from [11, Theorem 2.14], where it serves a different purpose. Let $\gamma \in \mathbb{F}_q^*$ be fixed. An element $x \in \mathbb{F}_q^*$ satisfies the equation $x(1-x) = \gamma$ if and only if it satisfies the equation $(2x-1)^2 = 1-4\gamma$. Hence, the number of solutions of the equation $x(1-x) = \gamma$ in F_q^* is $1+\rho(1-4\gamma)$, where ρ denotes the (unique) quadratic character on $\mathbb{F}_q$. It follows that every element of $\mathbb{F}_q^*$ is represented either twice or zero times in the form $x(1-x)$, save for 4^{-1}, which is represented once. Consequently, the multiset $\{x(x-1) : x \in \mathbb{F}_q^*\}$ can be represented in the group ring $\mathbb{Z}[\mathbb{F}_q^*]$ by $2Y - 4^{-1}$.

Making use of Lemma 2.4.3, we see that

$$\begin{aligned}\chi(-1)K(\chi) &= \chi(-4)\sum_{x\in\mathbb{F}_q^*}\chi(x)\chi(1-x)\\ &= \chi(-4)\sum_{x\in\mathbb{F}_q^*}\chi(x(1-x)) = \chi(-4)\chi(2Y-4^{-1})\\ &= \chi(2S^c-(-1)) = 2\chi(S^c)-\chi(-1).\end{aligned}$$

So, we deduce that

$$\chi(S^c) = \frac{1}{2}\chi(-1)(K(\chi)+1). \quad \square$$

Note that it follows from Lemma 4.0.1 that the expression we have found for $\chi(S^c)$ is indeed an algebraic integer.

Chapter 5

Shift-inequivalent decimations of the SLCE sequences

In this chapter, we consider the problem of determining maximal sets of shift-inequivalent decimations of the SLCE sequences, or rather the equivalent problem of determining the multiplier groups of the SLCE almost difference sets.

The problem of determining the multiplier groups of these almost difference sets was considered in [62]. Let p be an odd prime, d a positive integer, and S an SLCE almost difference set in $\mathbb{F}_q^*$. The authors of [62] were able to show that $\langle p \rangle$ is a subgroup of the group H_0 of strong multipliers of S. Furthermore, they explicitly computed the multiplier groups of SLCE almost difference sets in a number of cases. They found that for most of the SLCE almost difference sets that they considered, $\langle p \rangle$ com-

prised the entire multiplier group. However, they did find a case in which $\langle p \rangle$ was actually a proper subgroup of the multiplier group: when $p = 3$ and $d = 2$, the multiplier group H of the SLCE almost difference set S is $(\mathbb{Z}/(3^2 - 1)\mathbb{Z})^* = \{1, 3, 5, 7\} \neq \{1, 3\} = \langle p \rangle$. The authors of [62] mention that the problem of determining the multiplier groups of the SLCE sequences seems to be a hard problem. Furthermore, it is noted in [6] that this problem is still open.

5.1 A necessary condition coming from Stickelberger's Theorem *

Notation 5.1.1. *For the remainder of this chapter, let p be an odd prime, d a positive integer, and $q = p^d$. Let S be an SLCE almost difference set defined on $\mathbb{F}_q^*$, and let T be a set of distinct coset representatives of $\langle p \rangle$ in $(\mathbb{Z}/(q-1)\mathbb{Z})^*$.*

We begin by showing how the result we proved in Section 4.4 can be used to recover a theorem of Lempel, Cohn, and Eastman [62].

Theorem 5.1.2. *$\langle p \rangle$ is a subgroup of the strong multiplier group of S.*

Proof (new). Let χ be a character on $\mathbb{F}_q^*$, and let i be a positive integer. Then, by Lemma 4.4.1 and the Child's Binomial Theorem,

$$\chi((S^c)^{(p^i)}) = \sigma_{p^i}(\chi(S^c)) = \frac{1}{2}\sigma_{p^i}(\chi(-1)(K(\chi) + 1))$$

$$= \frac{1}{2}\chi(-1)^{p^i}(\sum_{x\in\mathbb{F}_q^*}\chi(x^{p^i})\chi((1-x)^{p^i})+1) = \frac{1}{2}\chi(-1)(\sum_{x\in\mathbb{F}_q^*}\chi(x^{p^i})\chi((1-x^{p^i}))+1)$$

$$= \frac{1}{2}\chi(-1)(K(\chi)+1) = \chi(S^c).$$

It follows by Lemma 3.3.4 that $(S^c)^{p^i} = S^c$. Consequently, $S^{p^i} = S$. $\square$

As a result of Theorem 5.1.2, the problem of determining the multiplier group of S reduces to determining which elements of T are multipliers of S. To that end, we now establish a necessary condition for an element $t \in T$ to be a multiplier of S.

Theorem 5.1.3. *Let p be an odd prime, let d be a positive integer, and let $q = p^d$. Let S be an SLCE almost difference set over $\mathbb{F}_q$. Let T be a set of distinct coset representatives of $\langle p\rangle$ in $(\mathbb{Z}/(q-1)\mathbb{Z})^*$, and let $t \in T$ be a multiplier of S. Then the sets $S_0 = \{j \in T : d - \sum_{i=0}^{d-1}\{\lfloor\frac{2(j^{-1})'p^i}{q-1}\rfloor - 2\lfloor\frac{(j^{-1})'p^i}{q-1}\rfloor\} > 0\}$ and tS_0 are either identical or disjoint.*

Proof. Notice that t is also a multiplier of $D = 2(-1)S^c$ (where $2 \in \mathbb{Z}$ and $-1 \in \mathbb{F}_{q-1}^*$). So, there exists $g \in \mathbb{F}_{q-1}^*$ such that $D^{(t)} = gD$. Let P be a prime ideal lying over p in $\mathbb{Z}[\zeta_{q-1}]$. Recall that the Techimuller character χ_P can be treated as a character on $\mathbb{F}_{q-1}^*$. We have that

$$\chi_P(D^{(t)}) = \chi_P(g)\chi_P(D) = \zeta\chi_P(D) = \zeta(K(\chi_P)+1),$$

where ζ is some (not necessarily primitive) $(q-1)$th root of unity. But, we

also have that

$$\chi_P(D^{(t)}) = \sigma_t(\chi_P(D)) = \sigma_t(K(\chi_P) + 1) = \sigma_t(K(\chi_P)) + 1.$$

Consequently,

$$\sigma_t(K(\chi_P)) - \zeta K(\chi_P) = \zeta - 1. \tag{5.1.1}$$

Now, assume there is a prime ideal Q lying over p that contains both $K(\chi_P)$ and $\sigma_t(K(\chi_P))$. Then, by (5.1.1), $\zeta - 1 \in Q$. Note that ζ is a primitive mth root of unity for some m dividing $q-1$.

By Lemma 3.4.2, if m is a product of more than one prime, then $N(1-\zeta) = 1$, and it follows that $\zeta - 1$ is a unit. However, since $\zeta - 1 \in Q$, this implies that $Q = \mathbb{Z}[\zeta_{q-1}]$, which is a contradiction. On the other hand, if $m = \ell^s$, for some prime ℓ and some positive integer s, then by Lemma 3.4.2, $N(1-\zeta) = \ell^{\phi(q-1)/\phi(m)}$, and so $\ell^{\phi(q-1)/\phi(m)} \in Q$. But, since $\ell | m | (q-1)$, we have that $\gcd(p, \ell^{\phi(q-1)/\phi(m)}) = 1$. So, since $p \in Q$ also, the Euclidean Algorithm implies that $1 \in Q$. Once again, we get the contradiction that $Q = \mathbb{Z}[\zeta_{q-1}]$.

The remaining possibility is that $m = 1$, i.e. that $\zeta = 1$. In this case, 5.1.1 implies that $\sigma_t(K(\chi_P)) = K(\chi_P)$. So, if *any* prime ideal lying over $K(\chi_P)$ also lies over $\sigma_t(K(\chi_P))$, then *every* prime ideal lying over $K(\chi_P)$ also lies over $\sigma_t(K(\chi_P))$. Consequently, by Theorem 4.1.1, S_0 and tS_0 are either identical or disjoint. $\square$

It is known that -1 is never a multiplier of a nontrivial cyclic difference set [8, Theorem 3.3]. Interestingly, in the case that $p = 3$ and $d = 2$, -1 actually is a multiplier of S. Naturally, it is of interest to determine when S has -1 as a multiplier. However, at least in the case $d = 1$, it is easy to see that our condition *never* rules out -1 as a multiplier of S.

Let $d = 1$. In this case, the set S_0 has a particularly simple description: namely,

$$S_0 = \{j \in (\mathbb{Z}/(p-1)\mathbb{Z})^* : (j^{-1})' < (p-1)/2\}.$$

Hence, it is clear that $j \in S_0$ if and only if $(j^{-1})' < (p-1)/2$ if and only if $(-j^{-1})' > (p-1)/2$ if and only if $-j \notin S_0$. So, in this case, S_0 and $-S_0$ are disjoint and so our condition does not rule out -1 as a multiplier.

Fortunately, we do have another tool at our disposal to help determine whether -1 is a multiplier of S. For, if -1 is a multiplier of S, then for some $\tau = 1, ..., q-1$, $\mathcal{C}_{\mathbf{s},\mathbf{s}[-1]}(\tau) = q-1$. However, by Theorem 2.4.6, $\mathcal{C}_{\mathbf{s},\mathbf{s}[-1]}(\tau) \leq 4\sqrt{q}+5$. So, we must have that $q-1 \leq 4\sqrt{q}+5$, i.e. that $q-4\sqrt{q} \leq 6$. But, for $x > 4$, $x - 4\sqrt{x}$ is an increasing function, and for $q = 27$, $q - 4\sqrt{q} \approx 6.2$. So, if $q > 25$, then -1 is not a multiplier of S. It can be checked directly that for $q \leq 25$, -1 is a multiplier of S if and only if $q = 3$, $q = 5$, or $q = 9$. Thus, the following proposition is a direct consequence of the cross-correlation bound from [24].

Theorem 5.1.4. *-1 is a multiplier of S if and only if $q = 3$, 5, or 9.*

There is another case in which Theorem 5.1.3 is not applicable. Suppose again that $d = 1$; additionally, assume that $p \equiv 1 \pmod 4$. Note that $(p-1)/2 - 1 \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$. Furthermore, note that $(p-1)/2 - 1$ is its own inverse. For $j \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$, $((p-1)/2-1)j \in S_0$ if and only if $(((p-1)/2-1)j)^{-1})' < (p-1)/2$ if and only if $(((p-1)/2-1)j^{-1})' < (p-1)/2$ if and only if (since $(j^{-1})'$ is odd) $(j^{-1})' < (p-1)/2$ if and only if $j \in S_0$. So, $((p-1)/2)S_0 = S_0$: our condition does not rule out the possibility that $(p-1)/2 - 1 = (p-3)/2$ and $-((p-1)/2-1) = (p+1)/2$ are multipliers.

5.2 Multipliers of SLCE almost difference sets over prime fields *

As an application of Theorem 5.1.3, we shall prove that in the case $d = 1$, when $p \equiv 3 \pmod 4$, the multiplier group of S is trivial and when $p \equiv 1 \pmod 4$ and $p > 70^2 + 1$, the multiplier group of S is a proper subgroup of the group $\langle (p-3)/2, (p+1)/2 \rangle$ of order 4.

Notation 5.2.1. *Let* $S_1 := \{j \in (\mathbb{Z}/(p-1)\mathbb{Z})^* : j' < (p-1)/2\}$.

Lemma 5.2.2. *Let p be an odd prime, and let S be an SLCE almost difference set over $\mathbb{F}_p^*$. Let $t \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ be a multiplier of S not equal to ± 1. Then there exists $a \in S_1$ such that $aS_1 = S_1$ and $a \neq 1$.*

Proof. Since the multipliers of S form a group, t^{-1} is also a multiplier of S. Hence, by Theorem 5.1.3, $t^{-1}S_0 = S_0$ or $t^{-1}S_0 \cap S_0 = \emptyset$.

Assume first that $t^{-1}S_0 = S_0$. Then for each $j \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$, $(j^{-1})' < (p-1)/2$ if and only if $(tj^{-1})' < (p-1)/2$. Hence, for each $j \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$, $(j)' < (p-1)/2$ if and only if $(tj)' < (p-1)/2$. Therefore, $S_1 = tS_1$. Furthermore, since $1 \in S_1$, $S_1 = tS_1$ implies $t \in S_1$.

Now assume that $t^{-1}S_0 \cap S_0 = \emptyset$. It then follows from the fact that $|-t^{-1}S_0| = |S_0| = |S_0^c|$ and the definition of S_0 that $-t^{-1}S_0 = S_0$. Thus, we can apply the above argument with "$-t$" in place of "t" to deduce that $S_1 = -tS_1$ (and that $-t \in S_1$). $\square$

As it turns out, the problem of deciding which elements $a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ $(a \neq 1)$ satisfy the equation $aS_1 = S_1$ is very similar to a problem which arises in the study of pure Jacobi sums. As we mentioned in Chapter 4, in [1], Akiyama determines the conditions under which Jacobi sums of the form $K(\chi)$ defined over $\mathbb{F}_{p^2}$ are pure. Like our work in this paper, Akiyama's work relies on Stickelberger's Theorem: indeed, he shows that a Jacobi sum is pure exactly when a condition holds that is almost identical to the necessary condition for a residue to be a multiplier given in Lemma 5.2.2.

Theorem 5.2.3. *Let p be an odd prime, let $k|p^2-1$, and let χ be a character on $\mathbb{F}_{p^2}$ of order k. Let $R_1 = \{x \in (\mathbb{Z}/k\mathbb{Z})^* : x' \in [1, k/2) \cap \mathbb{Z}\}$. Then $K(\chi)$ is pure if and only if there exists $a \in R_1$ such that $aR_1 = R_1$ and $p \equiv -a \pmod{k}$.*

As a result of the similarity between our condition and Akiyama's condition, we are able to apply the methods from [1] almost directly. Akiyama's

classification of pure Jacobi sums breaks into a number of cases, as does our study of the multiplier group of S over a prime field.

The proof of the following corollary is a straightforward modification of the proof of Lemma 4 in [1].

Corollary 5.2.4. *Let p be a prime congruent to 3 mod 4, and let S be an SLCE almost difference set over $\mathbb{F}_p^*$. Then the multiplier group of S is trivial.*

Proof. Let $t \neq \pm 1$ be a multiplier of S. Then, by Lemma 5.2.2, there exists $a \in S_1$ such that $a \neq 1$ and $aS_1 = S_1$. Pick an integer i such that

$$\frac{p-1}{2^{i+1}} < a' \tag{5.2.1}$$

and

$$a' \leq \frac{p-1}{2^i}. \tag{5.2.2}$$

Since $a \neq 1$, it follows from (5.2.2) that $(p-1)/2^{i+1} \geq 1$ and so that

$$2^i \leq (p-1)/2. \tag{5.2.3}$$

Since $p \equiv 3 \pmod 4$, there exists a congruence class $y \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ containing $(p-1)/2 - 2^i$. It follows from (5.2.3) that $y \in S_1$. Since a' is odd, we have that

$$a'\left(\frac{p-1}{2} - 2^i\right) \equiv \frac{p-1}{2} - 2^i a' \pmod{p-1}.$$

By (5.2.1) and (5.2.2),

$$\frac{p-1}{2} < 2^i a' \leq p-1.$$

Ergo, $ay \in S_1^c$. But this contradicts Lemma 5.2.2.

So, if t is a multiplier of S, then $t = \pm 1$. But, by Theorem 5.1.4, -1 is never a multiplier of S. Hence, the multiplier group of S is trivial. $\square$

The proof of the next result is a straightforward modification of the proof of Lemma 5 from [1].

Corollary 5.2.5. *Let p be a prime congruent to 1 mod 8 and greater than 14^2+1. Let S be an SLCE almost difference set over $\mathbb{F}_p^*$. Then the multiplier group of S is a proper subgroup of the group $\langle (p-3)/2, (p+1)/2 \rangle$ of order 4.*

Proof. Let $t \neq \pm 1, (p-3)/2, (p+1)/2$ be a multiplier of S. Then, by Lemma 5.2.2, there exists $a \in S_1$ such that $a \neq 1$ and $aS_1 = S_1$. For $c, d \in \mathbb{Z}^+$, set $T(c,d) = \{x \in (\mathbb{Z}/(p-1)\mathbb{Z})^* : x' \in [c,d) \cap \mathbb{Z}\}$, and for $j = 1,2,3,4$, set $T_j = T(((j-1)(p-1)/4, j(p-1)/4)$.

Note that since $(p-1)/2$ is even and a' is odd, there is a residue $y \in S_1$ containing $(p-1)/2 - a'$. Furthermore, since every integer belonging to a congruence class in S_1 is odd, the condition $aS_1 = S_1$ is equivalent to the condition $yS_1 = S_1$. Hence, we may assume $a \in T_1$. Indeed, since $t \neq \pm 1, (p-3)/2, (p+1)/2$, we can assume that $a' \in [3, (p-1)/4)$. Let us begin by assuming $a' \in [8, (p-1)/4) \cap \mathbb{Z}$.

Let i be the positive integer such that

$$a' \in \left[\frac{p-1}{2^{i+2}}, \frac{p-1}{2^{i+1}}\right). \tag{5.2.4}$$

Write $p-1 = 2^e m$, where $e \geq 3$ and m is odd. Let A, B, C, and D be elements of $(\mathbb{Z}/(p-1)\mathbb{Z})^*$ containing $(p-1)/2^e + 2^i$, $(p-1)/2^e + 2^{i+1}$, $(p-1)/2^e + (p-1)/4 + 2^i$, and $(p-1)/2^e + (p-1)/4 + 2^{i+1}$, respectively. Note that since $a' \leq (p-1)/2^{i+1}$ and $a' \geq 8$, we have that $2^{i+4} \leq 2^{i+1}a' \leq p-1$. Hence, $A, B, C, D \in S_1$.

Assume for the sake of contradiction that aA, aB, aC, and aD are all in S_1. First, note that

$$\left(\frac{p-1}{2^e} + 2^{i+1}\right) - \left(\frac{p-1}{2^e} + 2^i\right) = 2^i,$$

and by (5.2.4),

$$2^i a' \in \left[\frac{p-1}{4}, \frac{p-1}{2}\right).$$

Hence, $aB - aA \in T_2$. So, if $aA \in T_2$. then $aB \in T_3$ and so $aB \in S_1^c$, which contradicts our assumption. Thus, $aA \in T_1$, and $aB \in T_2$.

Since a' is odd, we consider the following two cases.

1) ($a' \equiv 1 \pmod 4$) In this case,

$$a'\left(\frac{p-1}{2^e} + \frac{p-1}{4} + 2^{i+1}\right) \equiv \frac{p-1}{4} + a'\left(\frac{p-1}{2^e} + 2^{i+1}\right) \pmod{p-1}.$$

Hence, since $aB \in T_2$, it follows that $aD \in T_3$ and so $aD \in S_1^c$, which contradicts our assumption.

2) ($a' \equiv 3 \pmod 4$) In this case,

$$a'\left(\frac{p-1}{2^e}+\frac{p-1}{4}+2^i\right) \equiv \frac{3(p-1)}{4}+a'\left(\frac{p-1}{2^e}+2^i\right) \pmod{p-1}.$$

Hence, since $aA \in T_1$, it follows that $aC \in T_4$ and so $aC \in S_1^c$, which contradicts our assumption. Thus, aA, aB, aC, and aD cannot all lie in S_1 simultaneously; the equation $aS_1 = S_1$ cannot be true.

It remains to consider the cases $a' = 3, 5, 7$. But, note that $aS_1 = S_1$ implies $a^2S_1 = S_1$. Also, $(p-1)/4 > 7^2$ implies that for each of these choices of a', $(a^2)' \in [8, (p-1)/4)$ and so the above argument can be applied to obtain a contradiction.

Thus, if t is a multiplier of S, then $t = \pm 1, (p-3)/2, (p+1)/2$. But, by Proposition 5.1.4, -1 is never a multiplier of S. Also, since the product of two multipliers is a multiplier and since $((p-3)/2)((p+1)/2) = -1$, it is not possible that both $(p-3)/2$ and $(p+1)/2$ are multipliers. Hence, the multiplier group of S is a proper subgroup of the group $\langle (p-3)/2, (p+1)/2 \rangle$ of order 4. $\square$

For proofs of the next three corollaries, see the proofs of Lemma 6, Lemma 7, and Lemma 8, respectively, in [1].

Corollary 5.2.6. *Let p be a prime satisfying $p-1 = 4m$ for some integer m*

such that $(m, 3) = 1$. *Let* p *be greater than* $10^2 + 1$. *Let* S *be an SLCE almost difference set over* $\mathbb{F}_p^*$. *Then the multiplier group of* S *is a proper subgroup of the group* $\langle (p-3)/2, (p+1)/2 \rangle$ *of order* 4.

Corollary 5.2.7. *Let* p *be a prime satisfying* $p - 1 = 4m$ *for some integer* m *which is odd and not square free. Let* p *be greater than* $46^2 + 1$. *Let* S *be an SLCE almost difference set over* $\mathbb{F}_p^*$. *Then the multiplier group of* S *is a proper subgroup of the group* $\langle (p-3)/2, (p+1)/2 \rangle$ *of order* 4.

Corollary 5.2.8. *Let* p *be a prime satisfying* $p-1 = 12m$ *for some integer* m *that has a prime factor greater than* 6. *Further assume that* $(m, 6) = 1$. *Let* p *be greater than* 70^2+1. *Let* S *be an SLCE almost difference set over* $\mathbb{F}_p^*$. *Then the multiplier group of* S *is a proper subgroup of the group* $\langle (p-3)/2, (p+1)/2$ *of order* 4.

Let S be an SLCE almost difference set over $\mathbb{F}_p^*$. Assume that $p > 70^2+1$. By Corollary 5.2.4, the multiplier group of S is trivial unless $4|(p-1)$. Assume $p - 1 = 4m$, for some integer m. By Corollary 5.2.5, the multiplier group of S is a proper subgroup of the group $\langle (p-3)/2, (p+1)/2 \rangle$ of order 4 unless m is odd. Assume m is odd. By Corollary 5.2.6, the multiplier group of S is a proper subgroup of the group $\langle (p-3)/2, (p+1)/2 \rangle$ unless $3|m$. So, assume $p - 1 = 12m'$, for some integer m'. By Corollaries 5.2.5 and 5.2.7, unless m' is square free and relatively prime to 6, then the multiplier group of S a proper subgroup of $\langle (p-3)/2, (p+1)/2 \rangle$. Assume m' is indeed square free and relatively prime to 6. Then, by Corollary 5.2.8, the multiplier group of

S is a proper subgroup of $\langle (p-3)/2, (p+1)/2 \rangle$, unless $m' = 5$, in which case $p < 70^2 + 1$, contradicting our assumption.

Hence, we have proven the following theorem.

Theorem 5.2.9. *Let p be an odd prime, let S be an SLCE almost difference set over $\mathbb{F}_p^*$, and let $\mathbf{s}$ be the periodic binary sequence corresponding to S. If $p \equiv 3 \pmod 4$, then the multiplier group of S is trivial, and $\mathcal{F}_1 = \{\mathbf{s}[t'] : t \in (\mathbb{Z}/(p-1)\mathbb{Z})^*\}$ is a family of $\phi(p-1)$ shift inequivalent decimations of $\mathbf{s}$. If $p > 70^2 + 1$ and $p \equiv 1 \pmod 4$, then the multiplier group of S is a proper subgroup of the group $\langle (p-3)/2, (p+1)/2 \rangle$ of order 4.*

Chapter 6

Progress towards determining the linear complexity of the SLCE sequences

In this chapter, we use our character formula to deduce information about the linear complexity of the SLCE sequences. The problem of determining the linear complexity of these sequences seems to be quite difficult, likely for the reason mentioned in Chapter 3: the SLCE sequences have even period. Over the past 15 years, several authors have attempted to solve this problem, and some progress has been made, but the problem is still open.

We begin by summarizing the state of the art prior to our work in this thesis, and then we turn to the task of using our character formula to deduce new information about the linear complexity of these sequences.

6.1 The state of the art

The problem of determining the linear complexity of the SLCE sequences was first considered by Helleseth and Yang [49] and subsequently taken up by Kyureghan and Pott [59] and finally by Meidl and Winterhof [73].

We recall the notation of Section 3.5.2. Let q be an odd prime power, $\mathbf{s} = s_0 s_1 s_2 ...$ an SLCE sequence over $\mathbb{F}_q^*$, and $S_2(x) := \sum_{i=0}^{q-2} s_i x^i \in \mathbb{F}_2[x]$. Each of the authors who have previously written on this problem have proceeded by attempting to determine the divisors of $\gcd(S_2(x), x^{q-1} - 1)$.

Let $k|q-1$, and let f be the order of k mod 2. Since $\mathbb{F}_{2^f}^*$ is a cyclic group of order $2^f - 1$, it has a subgroup of order k. Let $\beta \in \mathbb{F}_{2^f}$ be an element of order k, so that β is a root of $1 + x + \cdots + x^{k-1}$. Let $I_\beta(x)$ be the minimal polynomial of β over $\mathbb{F}_2$. We would like to determine whether or not $I_\beta(x)$ and/or $1 + x + \cdots + x^{k-1}$ divide $S_2(x)$. Furthermore, if $I_\beta(x)$ and/or $1 + x + \cdots + x^{k-1}$ do divide $S_2(x)$, we would like to determine the multiplicity with which they divide it.

Note that $I_\beta(x)|S_2(x)$ if and only if $S_2(\beta) = 0$, where $S_2(\beta)$ is an element of $\mathbb{F}_{2^f}$. For a polynomial $f(x) \in \mathbb{F}_2[x]$, let $f^{(t)}(x)$ denote the t-th formal derivative of $f(x)$. Note that $I_\beta(x)|S_2(x)$ with multiplicity t if and only if $S_2^{(t)}(\beta) = 0$.

The authors of all three papers mentioned above have used cyclotomic numbers to show that for certain elements β and certain values of t, $S_2^{(t)}(\beta) = 0$. Thus, they have been able to infer that under certain conditions, certain

polynomials divide $\gcd(S_2(x), x^{q-1}-1)$. The connection between cyclotomic numbers and expressions of the form $S_2^{(t)}(\beta)$ is given lucidly by the following equation from [73]. Assume that $q-1 = 2^\ell r$, for some odd number r. Then

$$S_2(\beta)^{(t)} = \sum_{h=0}^{r-1} \sum_{\substack{i=t \\ \binom{i}{t}=1}}^{2^\ell-1} \sum_{j=0}^{2^{\ell-1}r-1} (u(h,i), 2j+1)_{2^\ell r} \beta^h, \tag{6.1.1}$$

where $u(h,i)$ is the unique integer u such that $0 \leq u \leq 2^\ell r - 1$, $u \equiv h + k \pmod{r}$, and $u \equiv i \pmod{2^\ell}$. The applicability of (6.1.1) depends on whether or not one is able to evaluate the relevant cyclotomic numbers. As we mentioned in Section 3.1.1, explicit evaluations of cyclotomic numbers are known for cyclotomic numbers of small order. These evaluations generally depend on evaluations of Jacobi sums of small order. Consequently, most applications of (6.1.1) essentially amount to translations of the information from evaluations of Jacobi sums of small order into divisibility conditions for $S_2(x)$. There are certain other special cases in which evaluations of cyclotomic numbers are known, and these have also been exploited by the authors of [49], [59], and [73].

The authors of all three papers have used (6.1.1) to deduce conditions under which powers of $x+1$ divide $S_2(x)$. The most recent (and, consequently, most general) such conditions are given in [73]. The authors of [73] have deduced conditions under which certain other polynomials of low degree (such as $1 + x + x^2$) divide $S_2(x)$.

Kyureghan and Pott also made use of a different approach to finding divisors of $S_2(x)$. They proved the following result, which gives a criterion for determining whether certain polynomials divide $S_2(x)$ in terms of Jacobsthal sums in the case that $q \equiv 5 \pmod 8$ [59].

Theorem 6.1.1. *Let q be an odd prime such that $q = ef + 1$, where e is odd, and $4|f$. Let $\mathbf{s} = s_0 s_1 s_2 ...$ be an SLCE sequence over $\mathbb{F}_q^*$, and let $S_2(x) := \sum_{i=0}^{q-2} s_i x^i \in \mathbb{F}_2[x]$. Let α be a primitive element of $\mathbb{F}_q$. Then gcd$(S_2(x), x^{q-1} - 1)$ is divisible by $1 + x + \cdots + x^{e-1}$ if and only if*

$$I_e(1) \equiv -e \pmod 4,$$

and

$$I_e(\alpha^{-t}) \equiv 0 \pmod 4$$

for each $1 \leq t \leq e - 1$.

Under certain number theoretical hypotheses, Kyureghan and Pott are able to evaluate the congruences in Theorem 6.1.1 and thus obtain divisibility conditions for $\gcd(S_2(x), x^{q-1} - 1)$.

Thus, the authors of [49], [59], and [73] have obtained a number of theorems giving conditions under which certain polynomials divide $\gcd(S_2(x), x^{q-1} - 1)$. Each such result yields an upper bound on the linear complexity of certain classes SLCE sequences. Consequently, there is sufficient motivation to deduce more such results. In the next section, we use our character theorem

to derive divisibility results for the SLCE sequences different than the ones obtained in [49], [59], and [73]; the results we present all appeared in our recent paper [2].

We conclude this section by mentioning that Meidl and Winterhof have obtained a lower bound on the linear complexity of the SLCE sequences: in [73], they show that the linear complexity is always greater than or equal to $\sqrt{q} - 1$.

6.2 New divisibility conditions *

Once again, we fix the notation of Section 3.5.2 throughout this section. We assume that p is an odd prime, m is a positive integer, $q = p^m$, $\mathbf{s} = s_0 s_1 s_2 ...$ is an SLCE sequence over $\mathbb{F}_q^*$, and $S_2(x) := \sum_{i=0}^{q-2} s_i x^i \in \mathbb{F}_2[x]$.

Notation 6.2.1. *Let $k|q-1$ ($k \geq 3$) and let f be the order of k mod 2. Let $\beta \in \mathbb{F}_{2^f}$ be an element of order k, so that β is a root of $1 + x + \cdots + x^{k-1}$. Let $I_\beta(x)$ be the minimal polynomial of β over $\mathbb{F}_2$. Let $\mathcal{P}$ be a prime ideal lying over $\langle 2 \rangle$ in $\mathbb{Q}(\zeta_k)$.*

Using Condition 3.5.3 in concert with our character evaluation (Theorem 4.4.1) we deduce the following criterion for determining whether $I_\beta(x)$ divides $S_2(x)$.

Theorem 6.2.2. *We have*

$$I_\beta(x)|S_2(x) \iff \frac{1}{2}(K(\chi) + 1) \equiv 0 \pmod{\mathcal{P}}.$$

We use Theorem 6.2.2, in conjunction with the evaluations of the sums $K(\chi)$ given in Section 4.2, to obtain new results concerning the divisors of $\gcd(S_2(x), x^{q-1}+1)$. We first apply the evaluations of the pure Jacobi sums given in Corollary 4.2.7.

Lemma 6.2.3. *Suppose that there exist positive integers x satisfying the congruence $p^x \equiv -1 \pmod{k}$, and let t be the least such integer. Hence, by Theorem 4.2.4, $m = 2ts$ for some positive integer s.*

If $p \equiv 1 \pmod 4$, then $I_\beta(x)|S_2(x) \iff s \equiv 0 \pmod 2$.

If $p \equiv 3 \pmod 4$, then $I_\beta(x)|S_2(x) \iff$ either $s \equiv 0 \pmod 2$ or ts is odd.

Proof. By Corollary 4.2.7, $K(\chi)$ is pure; in fact, $K(\chi) \in \mathbb{Z}$. We know that $\mathcal{P} \cap \mathbb{Z} = 2\mathbb{Z}$ (see [3, Theorem 1.5.4]). Hence,

$$I_\beta(x)|S_2(x) \iff \frac{1}{2}(K(\chi)+1) \equiv 0 \pmod 2 \iff K(\chi)+1 \equiv 0 \pmod 4.$$

If $p \equiv 1 \pmod 4$, then by Corollary 4.2.7, we have

$$\begin{aligned} I_\beta(x)|S_2(x) &\iff (-1)^{1+(p^t+1)s/(2k)} p^{m/2} + 1 \equiv 0 \pmod 4 \\ &\iff (-1)^{1+(p^t+1)s/(2k)} + 1 \equiv 0 \pmod 4. \end{aligned}$$

Since k is odd, we have

$$I_\beta(x)|S_2(x) \iff (-1)^{1+s} + 1 \equiv 0 \pmod 4 \iff s \equiv 0 \pmod 2.$$

If $p \equiv 3 \pmod 4$, then by Corollary 4.2.7, we have

$$I_\beta(x)|S_2(x) \iff (-1)^{1+m/2+(p^t+1)s/(2k)}p^{m/2}+1 \equiv 0 \pmod 4.$$

We first assume that ts is even. Thus, $p^{m/2} \equiv 1 \pmod 4$. Hence,

$$I_\beta(x)|S_2(x) \iff (-1)^{1+(p^t+1)s/(2k)}+1 \equiv 0 \pmod 4.$$

If t is even and s is odd, then $1+(p^t+1)s/(2k) \equiv 0 \pmod 2$. On the other hand, if s is even, then $1+(p^t+1)s/(2k) \equiv 1 \pmod 2$. Hence, if ts is even, then

$$I_\beta(x)|S_2(x) \iff s \equiv 0 \pmod 2.$$

We now assume that ts is odd. Then

$$I_\beta(x)|S_2(x) \iff (-1)^{ts+(p^t+1)s/(2k)}+1 \equiv 0 \pmod 4 \iff (-1)+1 \equiv 0 \pmod 4.$$

So, clearly $I_\beta(x)|S_2(x)$ when ts is odd. $\square$

We use Lemma 6.2.3 to determine conditions under which

$$1+x+\cdots+x^{k-1} \mid S_2(x).$$

Theorem 6.2.4. *Suppose that there exist positive integers x satisfying the congruence $p^x \equiv -1 \pmod k$, and let t be the least such integer. Hence, by Theorem 4.2.4, $m = 2ts$ for some positive integer s.*

If $p \equiv 1 \pmod 4$, *then* $1 + x + \cdots + x^{k-1} | S_2(x) \iff s \equiv 0 \pmod 2$.

If $p \equiv 3 \pmod 4$, *then* $1+x+\cdots+x^{k-1} | S_2(x) \iff$ *either* $s \equiv 0 \pmod 2$ *or* ts *is odd.*

Proof. Let $\nu \in \mathbb{F}_q^*$ be an element of order n, where $n|k$. Since, $p^t \equiv -1 \pmod k$, it follows that $p^t \equiv -1 \pmod n$. Thus, the equation $p^x \equiv -1 \pmod n$ has a positive integer solution x. Let t' be the smallest such solution. There exists unique integers $y, r \geq 0$ such that $t = yt'+r$, $r < t'$. Furthermore,

$$-1 \equiv p^t = p^{yt'+r} \equiv (-1)^y p^r \pmod n.$$

Since $r < t'$, the above equation is only possible if $r = 0$. Hence, $t'|t$.

Now, by Theorem 4.2.4, there exists a positive integer s' such that $m = 2t's'$, so that $2t's' = 2ts = 2yt's$, and hence $s' = ys$. Consequently, we have

$$s \equiv 0 \pmod 2 \implies s' \equiv 0 \pmod 2.$$

Further, since $ts = t's'$, we have

$$ts \equiv 1 \pmod 2 \implies t's' \equiv 1 \pmod 2.$$

So, it follows from Lemma 4.1 that the conditions guaranteeing that $I_\beta(x)|S_2(x)$ are also sufficient to guarantee that $I_\nu(x)|S_2(x)$, where ν is any element of order dividing k. Thus, these conditions are sufficient to guarantee that $1 + x + \cdots + x^{k-1} | S_2(x)$. And, of course, they are also necessary. The

result follows. □

We now give some examples to illustrate Theorem 6.2.4.

Example 6.2.5. *Let* $p = 19$ *and let* $\mathbf{s}$ *be the SLCE sequence of length* $19^2 - 1 = 360$ *with corresponding polynomial* $S_2(x)$. *Note that* $5|20 = 19+1$. *Thus, we have* $p \equiv 3 \pmod 4$ *and* $s = t = 1$. *Hence,* ts *is odd. Thus,* Theorem 6.2.4 *guarantees that* $1 + x + x^2 + x^3 + x^4 | gcd(S_2(x), x^{360} + 1)$.

We use Theorem 6.2.4 to interpret some of the numerical results from [59].

Example 6.2.6. *Let* $q = 5^2$. *The authors of [59] found (via computer computations) that* $gcd(S_2(x), x^{q-1} + 1) = (x + 1)^4$. *Hence, even though* $3|5 + 1$, $1 + x + x^2 \nmid gcd(S_2(x), x^{q-1} + 1)$. *Of course, this follows from* Theorem 6.2.4 *since* $p \equiv 1 \pmod 4$, *but* $s = 1 \equiv 1 \pmod 2$.

Let $q = 3^4$. *Note that* $5|3^2+1$ *but* $5 \nmid 3+1$. *So,* $p \equiv 3 \pmod 4$, $t = 2$ *and* $s = 1$. *Hence,* $s \equiv 1 \pmod 2$ *and* ts *is even, so that* $1 + x + x^2 + x^3 + x^4 \nmid gcd(S_2(x), x^{q-1} + 1)$. *This agrees with the calculations in [59], where it was found that* $gcd(S_2(x), x^{q-1} + 1) = (x + 1)^{10}$.

Let $q = 5^4$. *Note that* $13|5^2 + 1$ *but* $13 \nmid 5 + 1$. *So,* $t = 2$, $s = 1$, *and* $p \equiv 1 \pmod 4$. *Since* $s \not\equiv 0 \pmod 2$, Theorem 6.2.4 *guarantees that* $1 + x + \cdots + x^{13} \nmid S_2(x)$. *This agrees with the calculations in [59], where it was shown that* $gcd(S_2(x), x^{q-1} + 1) = (x + 1)^{12}(x^2 + x + 1)^{10}$.

Let $q = 7^4$. *Note that* $5|7^2 + 1$. *So,* $t = 2$, $s = 1$, *and* $p \equiv 3 \pmod 4$. *By* Theorem 6.2.4, *since* $s \not\equiv 0 \pmod 2$ *and* ts *is even,* $1 + x + x^2 + x^3 +$

$x^4 \nmid S_2(x)$. *This agrees with the calculations in [59], where it was found that* $gcd(S_2(x), x^{q-1}+1) = (x+1)^{22}(x^2+x+1)^{18}(x^4+x+1)^2(x^4+x^3+1)^2$.

Let $q = 3^6$. *Note that* $7|3^3+1$. *So,* $t = 3$, $s = 1$, *and* $p \equiv 3 \pmod 4$. *Thus,* ts *is odd, and so* Theorem 6.2.4 *guarantees that* $1+x+\cdots+x^6 \mid S_2(x)$. *This agrees with the calculations in [59], where it was shown that*

$$\begin{aligned} &gcd(S_2(x), x^{q-1}+1) \\ &\quad = (x+1)^2(x^3+x+1)^4(x^3+x^2+1)^4(x^{12}+x^{11}+\cdots+x+1)^2 \\ &\quad = (x+1)^2(1+x+\cdots+x^6)^4(x^{12}+\cdots+x+1)^2. \end{aligned}$$

Let $q = 5^6$. *Now* $3|5+1$. *In this case,* $t = 1$, $s = 3$, *and* $p \equiv 1 \pmod 4$. *So, by* Theorem 6.2.4, $1+x+x^2 \nmid S_2(x)$. *Also,* $3^2|5^3+1$. *Here,* $t = 3$ *and* $s = 1$. *So, by* Theorem 6.2.4, $1+x+\cdots+x^8 \nmid S_2(x)$. *Finally,* $7|5^3+1$. *Here,* $t = 3$, *and* $s = 1$. *So, by* Theorem 6.2.4, $1+x+\cdots+x^6 \nmid S_2(x)$. *This agrees with the calculations in [59], where it was found that*

$$\begin{aligned} gcd(S_2(x), x^{q-1}+1) = (x^5+x^3+x^2+x+1)^4(x^5+x^4+x^3+x^2+1)^4 \\ \times(x^5+x^4+x^3+x+1)^4(x^5+x^4+x^3+x^2+1)^4. \end{aligned}$$

Let $q = 3^8$. *Now,* $5|3^2+1$. *Here,* $t = 2$, $s = 2$, *and* $p \equiv 3 \pmod 4$. *Hence, since* $s \equiv 0 \pmod 2$, Theorem 6.2.4 *guarantees that* $1+x+x^2+x^3+x^4|S_2(x)$. *Also,* $41|3^4+1$. *Here,* $t = 4$, *and* $s = 1$. *Hence, since* $s \not\equiv 0 \pmod 2$ *and since* ts *is even,* Theorem 6.2.4 *guarantees that* $1+x+\cdots+x^{40} \nmid S_2(x)$. *This*

agrees with the calculations in [59], where it was shown that

$$gcd(S_2(x), x^{q-1}+1) = (x+1)^{26}(x^4+x^3+x^2+x+1)^{18}.$$

We now apply the evaluations of the Jacobi sums of index 2 given in Corollary 4.2.10 to deduce new divisibility conditions.

Lemma 6.2.7. *Let $k = \ell^r$, where ℓ is a prime congruent to* 7 (mod 8) *and r is a positive integer. We suppose that $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle] = 2$ and $m = \phi(k)s/2$, where s is a positive integer. Let $e = \phi(k)/2$, so that $m = es$. Let a and b be determined as in Theorem 4.2.8 (Langevin's result).*

If $p \equiv 1 \pmod 4$, then

$$I_\beta(x) | S_2(x) \iff (-1)^{s-1-(p-1)s/4} \left(\frac{a+b}{2}\right)^s \equiv 3 \pmod 4.$$

If $p \equiv 3 \pmod 4$, then

$$I_\beta(x) | S_2(x) \iff (-1)^{s-1-rs+es+(1-h)s/2} \left(\frac{a+b}{2}\right)^s \equiv 3 \pmod 4.$$

Proof. Since $\ell \equiv 3 \pmod 4$, Theorem 3.4.4 implies that $K(\chi) \in \mathbb{Q}(\sqrt{-\ell})$. Since $\mathcal{P}$ is a prime ideal lying over 2, $\mathcal{P} \cap \mathbb{Q}(\sqrt{-\ell})$ is a prime ideal of $\mathbb{Q}(\sqrt{-\ell})$ lying over 2 (and conversely, for every prime ideal $\mathcal{P}'$ of $\mathbb{Q}(\sqrt{-\ell})$ lying above 2, there is a prime ideal $\mathcal{Q}$ of $\mathbb{Q}(\zeta_k)$ lying above 2 for which $\mathcal{Q} \cap \mathbb{Q}(\sqrt{-\ell}) = \mathcal{P}'$). Also, note that the procedure we have outlined in this chapter allows us free choice as to which prime ideal of $\mathbb{Q}(\zeta_k)$ lying above 2 we choose as $\mathcal{P}$. Finally,

recall that an explicit description of the prime ideals lying above 2 in $\mathbb{Q}(\sqrt{-\ell})$ is given in Theorem 3.4.6. Without loss of generality, let us choose $\mathcal{P}$ so that

$$\mathcal{P} \cap \mathbb{Q}(\sqrt{-\ell}) = \langle 2, \frac{-1+\sqrt{-\ell}}{2} \rangle.$$

In what follows, we will use the fact, mentioned above under Theorem 4.2.8, that $a \equiv b \pmod 2$ (where a and b are determined as in Theorem 4.2.8) as well as the simple facts that

$$\frac{1}{2}(K(\chi)+1) \equiv 0 \pmod{\mathcal{P}} \iff K(\chi)+1 \equiv 0 \pmod{2\mathcal{P}}$$

and that the squares mod 8 are congruent to either 0, 1, or 4.

Since $p \equiv 1, 3 \pmod 4$, it follows that $p^h \equiv 1, 3 \pmod 4$. Hence, $4p^h \equiv 4 \pmod 8$. If a and b are both odd, then $a^2, b^2 \equiv 1 \pmod 8$. So, if we assume that this is the case, then by Theorem 4.2.8,

$$4 \equiv 4p^h = a^2 + \ell b^2 \equiv 1 + 7 \cdot 1 \equiv 0 \pmod 8,$$

which is clearly impossible. Consequently, $a, b \equiv 0 \pmod 2$.

Case 1: $p \equiv 1 \pmod 4$. By Corollary 4.2.10, we have

$$\begin{aligned} K(\chi)+1 &= 1 + (-1)^{s-1-(p-1)s/4} p^{(e-h)s/2} \left(\frac{a+b\sqrt{-\ell}}{2}\right)^s \\ &= 1 + (-1)^{s-1-(p-1)s/4} p^{(e-h)s/2} \left(\frac{a+b}{2} + b\left(\frac{-1+\sqrt{-\ell}}{2}\right)\right)^s. \end{aligned}$$

Now, since $2\mathcal{P}|\langle 4\rangle$, it follows that $p^{(e-h)s/2} \equiv 1 \pmod{2\mathcal{P}}$. Further, since $b \equiv 0 \pmod 2$ and since, by Theorem 3.4.5, $\frac{-1+\sqrt{-\ell}}{2} \in \mathbb{Z}[\sqrt{n}]$, we have that $b\left(\frac{-1+\sqrt{-\ell}}{2}\right) \equiv 0 \pmod{2\mathcal{P}}$. Hence,

$$K(\chi) + 1 \equiv 1 + (-1)^{s-1-(p-1)s/4}\left(\frac{a+b}{2}\right)^s \pmod{2\mathcal{P}}.$$

But $1 + (-1)^{s-1-(p-1)s/4}\left(\frac{a+b}{2}\right)^s \in \mathbb{Z}$, and $2\mathcal{P} \cap \mathbb{Z} = \langle 4\rangle$. Consequently,

$$I_\beta(x)|S_2(x) \iff (-1)^{s-1-(p-1)s/4}\left(\frac{a+b}{2}\right)^s \equiv 3 \pmod 4.$$

Case 2: $p \equiv 3 \pmod 4$. By Corollary 4.2.10, we have

$$\begin{aligned} K(\chi)+1 &= 1 + (-1)^{s-1-rs+(e+1)s/2}p^{(e-h)s/2}\left(\frac{a+b\sqrt{-\ell}}{2}\right)^s \\ &= 1 + (-1)^{s-1-rs+(e+1)s/2}p^{(e-h)s/2}\left(\frac{a+b}{2} + b\left(\frac{-1+\sqrt{-\ell}}{2}\right)\right)^s. \end{aligned}$$

Now, since $2\mathcal{P}|\langle 4\rangle$, it follows that $p^{(e-h)s/2} \equiv (-1)^{(e-h)s/2} \pmod{2\mathcal{P}}$. Further, since $b \equiv 0 \pmod 2$ and since, by Theorem 3.4.5, $\frac{-1+\sqrt{-\ell}}{2} \in \mathbb{Z}[\sqrt{n}]$, we have that $b\left(\frac{-1+\sqrt{-\ell}}{2}\right) \equiv 0 \pmod{2\mathcal{P}}$. Hence,

$$K(\chi) + 1 \equiv 1 + (-1)^{s-1-rs+es+(1-h)s/2}\left(\frac{a+b}{2}\right)^s \pmod{2\mathcal{P}}.$$

But $1 + (-1)^{s-1-rs+es+(1-h)s/2}\left(\frac{a+b}{2}\right)^s \pmod{2\mathcal{P}} \in \mathbb{Z}$, and $2\mathcal{P} \cap \mathbb{Z} = \langle 4\rangle$.

Consequently,

$$I_\beta(x)|S_2(x) \iff (-1)^{s-1-rs+es+(1-h)s/2}\left(\frac{a+b}{2}\right)^s \equiv 3 \pmod 4. \quad \square$$

Let us now focus on the special case in which $r = 1$, so that $k = \ell$.

Theorem 6.2.8. *Let $\ell \equiv 7 \pmod 8$ be a prime, and let $k = l$. We suppose that $[(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle] = 2$ and $m = \phi(k)s/2$, where s is a positive integer. Let $e = \phi(k)/2$, so that $m = es$. Let a and b be determined as in Theorem 4.2.8 (Langevin's result).*

If $p \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$, then

$$1 + x + \cdots + x^{\ell-1}|S_2(x) \iff (-1)^{s-1-(p-1)s/4}\left(\frac{a+b}{2}\right)^s \equiv 3 \pmod 4.$$

If $p \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 4$, then

$$1+x+\cdots+x^{\ell-1}|S_2(x) \iff (-1)^{s-1-rs+es+(1-h)s/2}\left(\frac{a+b}{2}\right)^s \equiv 3 \pmod 4.$$

Proof. Note that $1+x+\cdots+x^{\ell-1}$ is the product of the minimal polynomials of the elements of $\mathbb{F}_{2^f}$ of order ℓ. So, if we can guarantee that the relevant condition from Lemma 4.2 is the same for each element β of order ℓ, then we can deduce conditions under which $1 + x + \cdots + x^{\ell-1}|S_2(x)$.

The explicit conditions given in Theorem 4.2.8 are sufficient to determine a completely and to determine b up to sign. In order to determine the sign of b, one must use Stickleberger's congruence [30, Lemma 3.5]. However,

we cannot guarantee that the sign of b will be same for Gauss/Jacobi sums corresponding to different characters of order k [11, Section 11.2]. But, if we assume that $b \equiv 0 \pmod 4$, then the residue class mod 4 of $\frac{a+b}{2}$ is unaffected by the sign of b. $\square$

We now give an example to illustrate Theorem 6.2.8.

Example 6.2.9. *Let* $\ell = 23 \equiv 7 \pmod 8$, *let* $p = 13 \equiv 1 \pmod 4$, *and let* $s = 1$. *It is easy to check that* $[(\mathbb{Z}/23\mathbb{Z})^* : \langle 13 \rangle] = 2$. *In this case,* $m = \phi(23)/2 = 11$, *so that* $q = 13^{11}$. *Referring to the class number table on [3, p. 325], we see that* $h = h(\mathbb{Q}(\sqrt{-23})) = 3$. *Further,* $4p^h = 4 \cdot 13^3 = (74)^2 + 23 \cdot (12)^2$, *so that* $a = \pm 74$ *and* $b = \pm 12$, *and since* $a \equiv -2p^{\frac{1}{2}(m+h)} \pmod \ell$, *we have that* $a = 74$. *By* Theorem 6.2.8, *we have*

$$1 + x + \cdots + x^{22} | S_2(x) \iff (-1)^{1-1-(13-1)\cdot 1/4} \left(\frac{74 \pm 12}{2} \right) \equiv 3 \pmod 4$$

$$\iff -37 \equiv 3 \pmod 4.$$

But $-37 \equiv 3 \pmod 4$, *and so* $1 + x + \cdots + x^{22} | S_2(x)$.

We conclude with a few remarks regarding the applicability of Theorem 6.2.8. The fastest way to compute the class number of $\mathbb{Q}(\sqrt{-\ell})$ is via an algorithm due to Shanks, which requires at most $O(\ell^{1/4+\epsilon})$ operations, where ϵ is any positive number; see [21, Section 5.4]. The class number of $\mathbb{Q}(\sqrt{-\ell})$ can be used to obtain divisibility results whenever p satisfies $[(\mathbb{Z}/\ell\mathbb{Z})^* : \langle p \rangle] = 2$, and it follows by Dirichlet's Theorem on primes in an

arithmetic progression that there are infinitely many primes p for which this is true. When the class number $h = 1$, there exists a probabilistic polynomial time algorithm, known as the modified Cornacchia algorithm, that can be used to find the integers a and b satisfying $4p^h = 4p = a^2 + \ell b^2$; see [21, Section 1.5.2]. In the general case, Hardy, Muskat, and Williams have given a deterministic algorithm that finds a and b (up to sign) in at most $O((4p^h)^{1/4}(\log 4p^h)^3(\log\log 4p^h)(\log\log\log(4p^h)))$ operations [45].

Chapter 7

Future work

We conclude this thesis by listing some open problems and formulating some research proposals concerning Sidelnikov sequences. This list is not comprehensive. Rather, it is a short list comprised of questions of particular interest to the author.

7.1 General questions

1) Ming Su has recently proposed an analogue of the Sidelnikov sequences in rings of the form $\mathbb{Z}/p(q-1)\mathbb{Z}$, where p is an odd prime, q is a power of an odd prime, and $\gcd(p,q) = 1$ [89]. Furthermore, Su obtains some partial results concerning the linear complexity of these sequences [89].

Is it possible to obtain more insight into the linear complexity of these sequences? Furthermore, can one determine what other randomness properties

they possess?

2) Are Su's new sequences the natural generalization of Sidelnikov sequences to residue rings not isomorphic to multiplicative groups of finite fields? Are there other interesting generalizations that might be considered? For instance, the generalized cyclotomic difference sets (and almost difference sets) are constructed in rings of the form $\mathbb{Z}_{pq}$, where p and q are odd primes and $\gcd(p, q) = 1$. Can one define an analogue of the Sidelnikov sequences in rings of this type? Of course, if new analogues could be defined, it would be interesting to try to determine their randomness properties.

3) What are the run properties of the Sidelnikov sequences?

4) The formula for the character values of the SLCE sequences given in Theorem 4.4.1 is similar to the formula for the character values of the hyperoval difference sets given in Equation 4.4.2. Is there an interesting geometric interpretation one could give for the Sidelnikov sequences? If so, does this geometric interpretation yield any insight into the pseudorandomness properties of these sequences?

7.2 Questions about decimations

5) What is the generalization of Theorem 4.4.1 from binary Sidelnikov sequences to M-ary Sidelnikov sequences? If one could compute character values of M-ary Sidelnikov sequences, would it be possible to say anything about the prime ideal factorization of the ideals generated by these character

values? In other words, is it be possible to prove an analogue of Theorem 5.1.3 for M-ary Sidelnikov sequences?

6) As we mentioned in Chapter 2, in certain special cases it is possible to compute the cross-correlation of two decimations of an m-sequence. Are there cases in which one could explicitly compute the cross-correlation of two decimations of a Sidelnikov sequence? If so, would it be possible to use some of the decimations in question to enlarge the Sidelnikov families mentioned in Section 2.4.2 without sacrificing too much in the way of cross-correlation?

7) Is it possible to use Theorem 5.1.3 to determine the multiplier groups of SLCE sequences for $d > 1$?

7.3 Questions about linear complexity

8) Is it possible to generalize Theorem 4.4.1 to a formula for character values of group ring elements corresponding to formal derivatives of $S_2(x)$? If so, would it be possible to explicitly evaluate the resulting character sums in certain special cases, as we were able to do with the sums arising from Theorem 4.4.1, and thereby determine the multiplicity with which certain polynomials divide $\gcd(S_2(x), x^{q-1} - 1)$?

9) Evans et al use (4.4.2) in conjunction with Stickelberger's Theorem and Theorem 3.5.1 to determine the linear complexity of the sequences corresponding to Maschietti's hyperoval difference sets. Is it possible to do something similar with SLCE sequences (at least to the extent of determin-

ing which polynomials divide $\gcd(S_2(x), x^{q-1} - 1)$, if not also determining the multiplicity with which they divide it)?

There are at least two possible complications that would need to be overcome. Firstly, equation 4.4.2 expresses the character values of the hyperoval almost difference sets as multiples of Jacobi sums. Thus, Stickelberger's Theorem and Theorem 3.5.1 provide a clear path towards studying the linear complexity of these sequences. But Theorem 4.4.1 describes the character values of the SLCE sequences as sums of the form $\frac{1}{2}(K(\chi) + 1)$. The "+1" part of this expression somewhat complicates matters.

Secondly, the authors of [29] actually compute the linear complexities in question by representing the exponents coming from Stickelberger's theorem as vectors of zeroes and ones and then performing computations with these vectors. They are able to obtain this representation of the exponents in question because the hyperoval difference sets are defined over finite fields of characteristic two. To represent the exponents given by Stickelberger's theorem for Jacobi sums over a finite field of characteristic p, one would have to make use of vectors with components from $\mathbb{F}_p$. Thus, the complexity of such computations increases along with the characteristic of the finite field one is working over.

So, it may turn out not be feasible to use the method from [29] to study SLCE sequences in the general case. However, it seems possible that it might bear fruit for low values of p.

Bibliography

[1] S. Akiyama, *On the pure Jacobi sums,* Acta Arithmetica **LXXV.2** (1996) 97-104.

[2] S. Alaca and G. Millar, *Character values of the Sidelnikov-Lempel-Cohn-Eastman Sequences,* Cryptography and Communications **9** (2017) no. 6, 665-682.

[3] S. Alaca and K. Williams, *Introductory algebraic number theory,* Cambridge UP (2003).

[4] H. Aly and W. Meidl, *On the linear complexity and k-error linear complexity over $\mathbb{F}_p$ of the d-ary Sidelnikov sequence,* IEEE Transactions on Information Theory **IT-53** (2007) no. 12, 4755-4761.

[5] H, Aly and A. Winterhof, *On the k-Error Linear Complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov Sequences,* Designs, Codes, and Cryptography **40** (2006) no. 3, 369-374.

[6] K. T. Arasu, C. Ding, T. Helleseth, V. Kumar, and H. M. Martinsen, *Almost difference sets and their sequences with optimal autocorrelation,* IEEE Transactions on Information Theory **IT-47** (2001) no. 7, 2934-2943.

[7] U. Bartocci and B. Segre, *Ovali ed altre curve nei piani di Galois di caratteristica due,* Acta Arithmetica **8** (1971) 423-449.

[8] L. D. Baumert, *Cyclic difference sets,* Springer-Verlag, New York (1971).

[9] E. R. Berlekamp, *Algebraic coding theory,* McGraw-Hill, New York (1968).

[10] B. C. Berndt and R. J. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer,* Illinois Journal of Mathematics **23** (1979) no. 3, 374-437.

[11] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums,* A Wiley-Interscience Publication (1998).

[12] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory,* 2nd Edition, Cambridge UP (1998).

[13] T. Beth and F. Piper, *The stop and go generator,* EUROCRYPT (1984), 88-92.

[14] A. Beutelspacher and U. Rosenbaum, *Projective geometry: from foundations to applications,* Cambridge UP (1998).

[15] N. Brandstätter and W. Meidl, *On the linear complexity of Sidelnikov sequences over* $\mathbb{F}_{q^d}$*,* Sequences and their applications - SETA 2006, Lecture Notes in Computer Science, **4086,** Springer, Berlin (2006) 47-60.

[16] N. Brandstätter, W. Meidl, and A. Winterhof *Addendum to Sidel'nikov Sequences Over Nonprime Fields,* Information Processing Letters, **113** (2006), 332-336.

[17] N. Brandstätter and A. Winterhof, *k-error linear complexity over* $\mathbb{F}_p$ *of subsequences of Sidelnikov sequences of period* $(p^r - 1)/3$*,* Journal of Mathematical Cryptology **3** (2009) no. 3, 215-225.

[18] J. H. Chung and K. Yang, *Bounds on the linear complexity and the 1-error linear complexity over* $\mathbb{F}_p$ *of M-ary Sidelnikov sequences,* Sequences and their applications - SETA 2006, Lecture Notes in Computer Science, **4086,** Springer, Berlin (2006) 74-87.

[19] R. Churchhouse, *Codes and ciphers: Julius Caesar, the Enigma, and the Internet,* Cambridge UP, Cambridge (2002).

[20] H. S. M. Coxeter, *Projective Geometry (2nd ed.),* Springer, New York (1987).

[21] H. Cohen, *A course in computational algebraic number theory,* Springer-Verlag, Berlin (1993).

[22] S. Chowla, *A property of biquadratic residues,* Proc. Nat. Acad. Sci. India **14** (1944), 45-46.

[23] H. Chung, J. S. Chung, Y. S. Kim, and J. S. No, *New families of of M-ary sequences with low correlation from Sidel'nikov sequences,* IEEE Transactions on Information Theory **IT-54** (2008) no. 8, 3768-3774.

[24] H. Chung, J. S. Chung, and J. S. No, *A construction of a new family of M-ary sequences with low correlation from Sidel'nikov sequences,* IEEE Transactions on Information Theory **IT-57** (2011) no. 4, 2301-2305.

[25] Hans Delfs and Helmut Knebl, *Introduction to cryptography: principles and applications,* Springer, Berlin (2007).

[26] Dummit and Foote, *Abstract Algebra,* Cambridge UP (1977).

[27] J. Eichstadt and C. F. Wedaman, *SINGCARS frequency hopping multiplexer,* Proceedings of the tactical communications conference. Tactical communications: technology in transition. **1** Fort Wayne, IN, USA (1992) 125-131.

[28] Bruce R. Elbert, *The satellite communication applications handbook, 2nd ed.* Artech House, Boston (2004).

[29] R. Evans, H. D. L. Hollmann, C. Krattenthaler, and Q. Xiang, *Gauss Sums, Jacobi Sums, and p-Ranks of Cyclic Difference Sets,* Journal of Combinatorial Theory, Series A **87** (1999) 74-119.

[30] T. Feng and Q. Xiang, *Cyclotomic constructions of skew Hadamard difference sets,* Journal of Combinatorial Theory, Series A **119** (2012) 245-256.

[31] J. Gallian, *Abstract Algebra,* Cambridge UP (1977).

[32] R. Games, *The geometry of m-sequences: three-valued cross-correlations and quadrics in finite projective geometry,* SIAM J. Alg. Disc. Meth. **7** (1986) 43-52.

[33] C. F. Gauss, *Theorim residuoroum biquadraticorum, commentatio prima,* Comment. Soc. Reg. Sci. Gottingenis **6** (1828) 65-92.

[34] M. Z. Garaev, F. Luca, I. E. Shparlinski, and A. Winterhof, *On the Lower Bound of the Linear Complexity over $\mathbb{F}_p$ of Sidelnikov Sequences,* IEEE Transactions on Information Theory **IT-52** (2006) no. 7, 3299-3304.

[35] D. G. Glynn, *Two new sequences of ovals in finite Desarguesian planes of even order. In: Combinatorial Mathematics (ed. L. R. A. Case)* Springer, New York (1983) 217-229.

[36] R. Gold, *Maximal recusive sequences with 3-valued recursive cross-correlation functions,* IEEE Transactions on Information Theory **IT-14** (1968) 154-156.

[37] S. W. Golomb *Sequences with randomness properties,* Baltimore Glenn L. Martin Company (1977).

[38] S. W. Golomb *Shift register sequences,* Holden-Day (1967).

[39] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar,* Cambridge UP (2005).

[40] G. Gong and N. Y. Yu, *New construction of m-ary sequence families with low correlation from the structure of the Sidelnikov sequences,* IEEE Transactions on Information Theory **IT-56** (2010) no. 8, 4061-4070.

[41] B. Gordon, W. H. Mills, and L. R. Welch, *Some new difference sets,* Canadian Journal of Mathematics **14** (1962) 614-625.

[42] M. Goresky and A. Klapper, *Algebraic shift register sequences,* Cambridge UP (2012).

[43] M. Hall, Jr. *Cyclic projective planes,* Duke Journal of Mathematics **14** (1947) 1079-1090.

[44] M. Hall, Jr. *A survey of difference sets,* Proceedings of the American Mathematical Society **7** (1956) 975-986.

[45] K. Hardy, J. B. Muskat, and K. S. Williams, *A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v,* Math. Comp. **55** (1990) no. 91, 327-343.

[46] T. Helleseth, *Some results about the cross-correlation function between two maximal length linear sequences,* Discrete Math **16** (1976) 209-232.

[47] T. Helleseth, S. H. Kim, and J. S. No, *Linear Complexity over $\mathbb{F}_p$ and Trace Representation of Lempel-Cohn-Eastman Sequences,* IEEE Transactions on Information Theory **IT-49** (2003) no. 6, 1548-1552.

[48] T. Helleseth, M. Maas, J. E. Mathiassen, and T. Segers, *Linear Complexity Over $\mathbb{F}_p$ of Sidel'nikov Sequences,* IEEE Transactions on Information Theory **IT-50** (2004) no. 10, 2468-2472.

[49] T. Helleseth and K. Yang, *On binary sequences of period $n = p^m - 1$ with optimal autocorrelation,* Proceedings of SETA01 (T. Helleseth, P. Kumar, and K. Yang, eds.) (2002) 209-217.

[50] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions (2nd ed.),* Oxford UP, Oxford (1998).

[51] K. Horadam, *Hadamard matrices and their applications,* Princeton UP (2007).

[52] ed. F. Hu, *Opportunities in 5G: a research and development perspective,* CRC Press (2016).

[53] K. Ireland and M. Rosen, *A classical introduction to modern number theory,* 2nd Edition Springer-Verlag (1990).

[54] ed. E. D. Kaplan, *Understanding GPS: principles and applications,* Artech House, Boston (1996).

[55] J. F. Keating, *A cositable ground radio for HAVE QUICK and SATURN,* Proceedings of the tactical communications conference. Tactical communications: challenges of the 1990s. **1** Fort Wayne, IN, USA (1990) 569-591.

[56] Y. S. Kim, J. S. Chung, J. S. No, and H. Chung, *Linear complexity over $\mathbb{F}_p$ of ternary Sidelnikov sequences,* Sequences and their applications - SETA 2006, Lecture Notes in Computer Science, **4086,** Springer, Berlin (2006) 61-73.

[57] Y. T. Kim, D. San, and H. Y. Song, *New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences,* IEEE Transactions on Information Theory **IT-61** (2015) no. 1, 655-670.

[58] N. Koblitz, *A course in number theory and cryptography,* Springer-Verlag, New York (1994).

[59] G. M. Kyureghyan and A. Pott, *On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences,* Designs, Codes, and Cryptography **29** (2003) 149-164.

[60] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes,* IEEE Transactions on Information Theory **36** (1990) 686-692.

[61] P. Langevin, *Calculs de Certaines Sommes de Gauss,* Journal of Number Theory **63** (2003) 59-64.

[62] A. Lempel, M. Cohn, and W. L. Eastman, *A class of balanced binary sequences with optimal autocorrelation properties,* IEEE Transactions on Information Theory **IT-23** (1977) no. 1, 38-42.

[63] E. Lehmer, *On residue difference sets,* Canadian Journal of Mathematics **5** (1953) 425-432.

[64] K. H. Leung and B. Schmidt, *The field descent method,* Designs, Codes, and Cryptography (2003) 59-64.

[65] W. J. Leveque Fundamentals of number theory Dover, New York1977.

[66] R. Lidl and H. Niedereitter Finite fields Cambridge UP1996.

[67] S. L. Ma, *A survey of partial difference sets,* Designs, Codes, and Cryptography (1994) 221-261.

[68] J. MacWilliams and H. B. Mann, *On the p-rank of the design matrix of a difference set,* Inform. Control **12** (1968) 474-488.

[69] H. B. Mann, *Introduction to algebraic number theory,* Ohio State Press, Columbus, Ohio (1955).

[70] A. Maschietti, *Difference sets and hyperovals,* Designs, Codes, and Cryptography **14** (1998) 89-98.

[71] J. L. Massey, *Shift register synthesis and BCH decoding,* IEEE Transactions on Information Theory **IT-15** (1969) 122-127.

[72] R. McEliece, *Finite fields for computer scientists and engineers,* Norwell, MA, Kluwer Academic Publishers (1977).

[73] W. Meidl and A. Winterhof, *Some Notes on the Linear Complexity of Sidel'nikov-Lempel-Cohn-Eastman Sequences,* Designs, Codes, and Cryptography **8** (2006) 159-178.

[74] G. Millar, *A class of mutually inequivalent circulant weighing matrices,* Australasian Journal of Combinatorics **54** (2012) 3-11.

[75] Understanding spread spectrum for communications, National Instruments white paper, Retrieved June 24, 2017 from: http://www.ni.com/white-paper/4450/en/.

[76] D. K. Nguyen and B. Schmidt, *Fast computation of Gauss sums and resolution of the root of unity ambiguity,* Acta Arithmetica **140**, no. 3 (2009) 205-232.

[77] R. E. A. C. Paley, *On orthogonal matrices* J. Math. Phys. **12** (1933) 311-320.

[78] S. E. Payne, *A complete determination of translation ovoids in finite Desarguesian planes,* Atti. Acad. Naz. Lincei Rend. **51** (1971) 328-331.

[79] J. Pieprzyk, T. Hardjono, and J. Seberry *Fundamentals of computer security,* Springer (2003).

[80] M. Pursley and D. Sarwate, *Cross-correlation properties of pseudorandom and related sequences,* Proceedings of the IEEE **68** (1987) 593-619.

[81] P. Ribenboim Algebraic numbers Wiley, New York1972.

[82] M. J. B. Robshaw, *Stream ciphers,* RSA Laboratories Technical Report **TR-701** (1995).

[83] B. Schmidt, *Cyclotomic integers and finite geometry,* Journal of the American Mathematical Society **12** (1999) 929-952.

[84] C. Shannon, *Communication theory of secrecy systems,* Bell Systems Technical Journal **28** (1949) no. 4, 656-715.

[85] K. Shiratani and M. Yamada, *On rationality of Jacobi sums,* Colloq. Math. **73** (1997) no. 2, 251-260.

[86] V. M. Sidelnikov, *Some k-valued pseudo-random sequences and nearly equidistant codes,* Probl. Inf. Transm. **5** (1969) 12-16.

[87] J. Singer, *A theorem of finite projective geometry and some applications to number theory,* Transactions of the American Mathematical Society **43** (1938) 377-385.

[88] T. Storer *Cyclotomy and difference sets,* Markham Publishing Company, Chicago (1967).

[89] M. Su, *On the linear complexity of Legendre-Sidelnikov sequences,* Designs, Codes, and Cryptography **74** (2015) 703-717.

[90] D. Torrieri *Principles of spread spectrum communication systems,* Springer (2015).

[91] R. J. Turyn, *Character sums and difference sets,* Pacific Journal of Mathematics **15** (1965) 319-346.

[92] H. E. Wanders, *On the significance of Golomb's randomness postulates in cryptography,* Philips J. Res. **43** (1988) 185-222.

[93] A. Weil, *Number of solutions of equations in a finite field,* Bull. Am. Math. Soc. **55** (1949) 497-508.

[94] L. R. Welch, *Lower bounds on the maximum correlation of signals,* IEEE Transactions on Information Theory **IT-20** (1974) 397-399.

[95] A. L. Whiteman, *A family of difference sets,* Illinois Journal of Mathematics **6** (1962) 107-121.

[96] F. W. Winterbotham, *The Ultra secret: the inside story of Operation Ultra, Bletchley Park and Enigma,* Orion Books Ltd, London (1974).

[97] L. Xia and J. Yang, *Complete Solving of Explicit Evaluation of Gauss Sums in the Index* 2 *Case,* Sci. China Math. **53** (2010) no. 9, 2525-2542.

[98] Q. Xiang, *Some results on multipliers and numerical multiplier groups of difference sets,* Graphs Comb. **10** (1994) 293-304.

[99] K. Yamamoto, *Decomposition fields of difference sets,* Pacific Journal of Mathematics **13** () no. 1, 38-42.

[100] N. Zierler, *Linearly recurring sequences,* J. Soc. Indust. Appl. Math. **7** (1959) 31-48.